A CHANGE OF DETECTION: TO FIND THE TERRORIST WITHIN THE IDENTIFICATION OF THE U.S. ARMY'S INSIDER THREAT

A thesis presented to the Faculty of the U.S. Army Command and General Staff College in partial fulfillment of the requirements for the degree

MASTER OF MILITARY ART AND SCIENCE
Homeland Security

by

CHRISTINE BAKER, MAJOR, U.S. ARMY
B.A., Virginia Commonwealth University, Richmond, VA 2000

Fort Leavenworth, Kansas
2012-01

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From-To)*
08-06-2012	Master's Thesis	AUG 2011 – JUN 2012

4. TITLE AND SUBTITLE
A Change of Detection: To Find the Terrorist within the Identification of the U.S. Army's Insider Threat

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Major Christine Baker

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
Fort Leavenworth, KS 66027-2301

8. PERFORMING ORG REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Thirteen individuals were killed and thirty-two individuals injured in the Fort Hood shooting. The U.S. Army bearing the wound left a nation questioning of how one of their own military members could be accused of such catastrophic events.

In the aftermath of reviews and Congressional testimony, there have been changes proposed for the identification of insider threats. The Federal Insider Threat Task Force is faced with developing the comprehensive program for all departments. In the interim, Congress proposes a significant challenge to the Departments to synchronize the efforts to identify insider threats to the United States. Prior to the Department of Defense synchronization, the U.S. Army has proposed changes within their forces to identify and define this insider threat. This thesis reviews the proposed U.S. Army identification processes in correlation to the Fort Hood shooting as a Homegrown Terrorism Threat. The purpose is to compare and analyze modifications that can best be applied to predicting and mitigating the homegrown terrorist segment of the U.S. Army's insider threat.

15. SUBJECT TERMS
Insider Threat, Homegrown Terrorism, Radicalization, Threat Detection

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. PHONE NUMBER** *(include area code)*
(U)	(U)	(U)	(U)	88	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: Major Christine M. Baker

Thesis Title: A Change of Detection: To Find the Terrorist within the Identification of the U.S. Army's Insider Threat

Approved by:

_____, Thesis Committee Chair
De Ette A. Lombard, M.A.

_____, Member
MG William D.R. Waff, D.Min.

_____, Member
William T. Pugh, M.A.

Accepted this 8th day of June 2012 by:

_____, Director, Graduate Degree Programs
Robert F. Baumann, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

A CHANGE OF DETECTION: TO FIND THE TERRORIST WITHIN THE IDENTIFICATION OF THE U.S. ARMY'S INSIDER THREAT, by Major Christine Baker, 88 pages.

Thirteen individuals were killed and thirty-two individuals were injured in the Fort Hood shooting. The U.S. Army bearing the wound left a nation questioning how one of their own military members could be accused of such catastrophic events.

In the aftermath of reviews and Congressional testimony, changes have been proposed for the identification of insider threats. A significant challenge resides in the Federal Government to synchronize the efforts to identify insider threats within the United States. Prior to the Assistant Secretary of Defense for Homeland Security synchronization, the U.S. Army proposed changes within their forces to identify and define this insider threat. This thesis reviews the proposed U.S. Army identification processes in correlation to the Fort Hood shooting. The purpose is to compare and analyze modifications that can best be applied to predicting and mitigating the homegrown terrorist segment of the U.S. Army's insider threat.

ACKNOWLEDGMENTS

I would like to thank my committee members, Ms. De Ette A. Lombard, MG William D. R. Waff and Mr. William T. Pugh, for being patient with me and teaching me a tremendous amount about research and clarity of the written word. You did not have to accept this challenge and yet you did. I can only hope that maybe my research helped you, although I acknowledge it will never compare to the amount of assistance you have given me. Thank you.

TABLE OF CONTENTS

Page

MASTER OF MILITARY ART AND SCIENCE THESIS APPROVAL PAGE iii

ABSTRACT iv

ACKNOWLEDGMENTS v

TABLE OF CONTENTS vi

ACRONYMS viii

ILLUSTRATIONS ix

TABLES x

CHAPTER 1 INTRODUCTION 1

The Problem Statement 2
Research Questions 4
Background 4
Insider Threat Defined 4
Identifying Insider Threat 8
Assumptions 10
Scope and Limitations 10
Scope 10
Limitations 11
Delimitations 12

CHAPTER 2 LITERATURE REVIEW 13

Research Questions 13
Determining the Insider Threat 15
The Homegrown Terrorism Threat to the Military 16
High Risk Individuals at the Expense of Manning the Force? 17
What Can Be Learned From the Fort Hood Shooting? 19
Testimony from Senator Joseph Lieberman on His Report of the Fort Hood Shooting 22
Officership Training Evaluation of the Army Medical Department Center and School 23
The Army Acknowledges Insider Threat is an Army Leadership Issue 24
Findings from U.S. Army Reports on the Fort Hood Shooting Conclude the Army Must Train Their Leaders 25

Identifying the Insider Threat 26
American Radicalized Threat 27
Applying a Multiple Echelon Approach to Identifying Insider Threats 29
The Reason Network Security Works for Identifying Insider Threats 30
Whitepaper on Simulation Information to Insider Threat Detection 31
The Layered Approach of Identifying Insider Threats Using a Scenario Based Approach 33
Modeling Software to Detect Insider Threats 35
Defense Software Modeling 37
The U.S. Army's Identification Processes 37
The Army Anti-Terrorism Identification Recommendations 37
Army Regulation (AR) 381-12, Threat Detection 39
The U.S. Army's Asymmetric Warfare Group Model for Identifying Insider Threats 41
Summary of Literature Review 43

CHAPTER 3 RESEARCH METHODOLOGY 44

Research Questions 45
The Research Evolution 45
Key Definitions: 48
The Approach 50
The Criteria of an Accurate Insider Threat Model 51

CHAPTER 4 ANALYSIS 55

Research Question 55
Results of Side-by-Side Comparison of the Three Models of Detecting Insider Threat 56
Research Difficulties 62

CHAPTER 5 CONCLUSIONS AND RECOMMENDATIONS 64

Research Questions 65
Conclusions 65
Answering the Research Questions 65
Discoveries That Emerged 67
Recommendations 70

GLOSSARY 72

BIBLIOGRAPHY 74

INITIAL DISTRIBUTION LIST 78

ACRONYMS

ADAMS	Anomaly Detection at Multiple Scales
AR	Army Regulation
ASD	Assistant Secretary of Defense
ATFP	Anti-Terrorism and Force Protection
AWG	Asymmetric Warfare Group
CERT	Computer Emergency Response Team
DARPA	Defense Advanced Research Projects Agency
DHS	Department of Homeland Security
DOD	Department of Defense
FBI	Federal Bureau of Investigations
HD & ASA	Homeland Defense and America's Security Affairs
MEDCOM	Medical Command
NPR	National Public Radio
SIM	Security Information Management, usually used in conjunction with the word System
TRADOC	Training and Doctrine Command
UCMJ	Uniform Code of Military Justice
U.S.	United States

ILLUSTRATIONS

Page

Figure 1 Model For Determining Insider Threat as Depicted in a Scenario-Based Approach to Mitigating the Insider Threat. 34

Figure 2 Insider Threat Detection Using Situation-Aware MAS. 36

Figure 3. The Lenses of Comparing the Army's Models of Insider Threat 52

TABLES

Page

Table 1. Profiling an Inside Attacker According to SANS White paper Results 32

Table 2. Insider Threat Detection Using Situation-Aware MAS Table.....36

Table 3. Army's ATFP Level 1 Identification Model of Insider Threat.....39

Table 4. Asymmetric Warfare Group Observable Indicators of Insider Threats.....42

Table 5. Comparing the Three Army Insider Threat Identification Processes 62

CHAPTER 1

INTRODUCTION

> The New America Foundation and the Maxwell School of Public Policy examined 192 cases of apparent homegrown terrorism by Islamist militants since 9-11. We found that the American military at home and abroad is indeed a target for Islamist extremist plots. In a third of the cases we studied, the individuals who were charged had targeted the U.S. military. Of those, a little under half targeted military facilities or personnel in the United States, while 55% were targeting American bases and troops overseas.[1]
>
> —Peter Bergeron, CNN

The New America Foundation defines homegrown terrorism as a U.S. citizen or refugee who intends to conduct attacks against the United States. Homegrown terrorism is a topic of significant discussion and study because of recent planned, attempted, and executed strikes of insider threats in the United States. Through case study analysis, the New America Foundation determined one of the primary targets within America over the past ten years is the U.S. military.[2]

Senator Joseph I. Lieberman, Independent from Connecticut, stated in an article on CNN.com that the threat of homegrown terrorism against the U.S. military has grown significantly since 2006.[3] Much of that threat stems from homegrown terrorists that are categorized as an insider threat existing within the United States. A large portion of the

---

[1]Peter Bergeron, "Measuring the Homegrown Threat to the Military," *CNN*. http://www.cnn.com/2011/12/07/opinion/bergen-terrorist-threat-military/index.html (accessed 7 December 2011).

[2]New America Foundation and Syracuse University's Maxwell School, "Homegrown Terrorism Cases, 2001-2011," http://homegrown.newamerica.net (accessed 13 March 2012).

[3]Bergeron.

threat is directed at the U.S. military. After reviewing the Maxwell School case studies, one case, commonly referred to as the Fort Hood shooting, demonstrated the targeted catastrophic consequences for the U.S. Army. It illustrates just how serious the homegrown terrorist threat is for the U.S. military.

The Fort Hood shooting refers to an attack by Major (Dr.) Nidal Malik Hasan, a physician who is a U.S Army officer, accused of "thirteen counts of pre-meditated murder and thirty-two counts of attempted murder" at a pre-deployment center at Fort Hood, Texas.[4] This case is one of the most recent examples of the U.S. Army's insider threat and demonstrates America's homegrown terrorist threat.

The Problem Statement

The U.S. media reported, "Although no single event directly led to the tragedy at Fort Hood, certain officers clearly failed to meet the high standards expected of their profession."[5] Several reports before the incident indicated that leaders in Major Hasan's chain of command had already identified him, as early as 2007, as unprofessional and possessing radical beliefs; however no actions were taken.[6] Even after, these issues were

[4]Phillip Jankowski, "Judge delays Hasan court-martial until June," *Killeen Daily Herald*, 2 February 2012, http://www.kdhnews.com/news/story.aspx?s=63990 (accessed 12 February 2012).

[5]Louis Martinez, "Army to Punish 9 Officers for Fort Hood Shootings," *ABC News*, http://abcnews.go.com/Politics/army-punish-officers-fort-hood-shootings/story?id=13109621 (accessed 25 February 2012).

[6]Opening statement of Senator Joseph I Lieberman of Connecticut, speaking before the hearing on A Ticking *Time Bomb: Counterterrorism Lessons from the U.S. Government's Failure to Prevent the Fort Hood Attack* on 15 February 2011 to the Committee on Homeland Security and Governmental Affairs 112th Congress, 1st sess. http://www.hsdl.org/?view&did=7760 (accessed 12 April 2012).

documented, he continued to serve, to be promoted, and to be assigned to a new duty station at Fort Hood, Texas. Major Hasan had been referred to the Federal Bureau of Investigations (FBI) for possible terrorist activity. The FBI confirmed that Major Hasan contacted a suspected terrorist, but they determined it had been for research purposes only.[7] Not until 5 November 2009 when the shooting occurred, did Major Hasan become known in America as a homegrown terrorist case.

As stated, even though Major Hasan's beliefs and behaviors were reported, no actions were taken. Major Hasan's trial is currently scheduled for 12 June 2012, where it is hoped many questions will be answered.[8] Meanwhile, his leaders have been criticized for not having taken action prior to the events on 5 November. Nine of Major Hasan's leaders have been criticized and admonished for not discharging him.[9]

Since 5 November 2009, there have been multiple reports and even Congressional testimony examining the events leading up to the Fort Hood shooting. Different agencies, within the U.S. Army, have made amendments to terminology to address insider threats and how to recognize these threats. This thesis will look at these proposed changes within the context of the Fort Hood shooting.

---

[7]Senator Joseph I. Lieberman of Connecticut, speaking before the hearing on A Ticking *Time Bomb: Counterterrorism Lessons from the U.S. Government's Failure to Prevent the Fort Hood Attack* on 15 February 2011 to the Committee on Homeland Security and Governmental Affairs 112th Congress, 1st sess. http://www.hsdl.org/?view&did=7760 (accessed 12 April 2012).

[8]Phillip Jankowski. "Judge delays Hasan court-martial until June," *Killeen Daily Herald*, 2 February 2012, http://www.kdhnews.com/news/story.aspx?s=63990 (accessed 12 February 2012).

[9]*Pittsburgh Post-Gazette*, "Ft. Hood officers face punishment," 15 January 2010, http://www.proquest.com.lumen.cgsccarl.com/ (accessed 25 February 2012).

Research Questions

As the U.S. Army works to improve its ability to identify and deter insider threats, this study will seek to discover the answer to the question: Do U.S. Army insider threat identification procedures enable leaders to accurately determine a homegrown insider threat like the threat of the Fort Hood shooting?

Background

The U.S. Army has conducted a multitude of after-action reviews on the Fort Hood shooting. Prior to the Fort Hood shooting, there was little study on the Army's insider threat. Additionally, the term insider threat did not appear in manuals or training until after the reviews on Fort Hood were concluded in 2010. Because insider threat is a relatively new area of concern for the U.S. Army, it is essential to define this term before conducting this study to ensure a shared understanding of the term and its threat to the military.

Insider Threat Defined

The definition of insider threat depends on what lens it is viewed through. Current definitions often define insider threat differently based on the organization that writes the definition. For example, U.S. Cyber Command uses a different definition than the U.S. Army's Military Intelligence community. To date, there is no definition of it in any of the Army leadership manuals.

Illustrating the differences of the definitions begins with a description of insider threat based on the Cyber Command definition of insider threat as depicted in a 2010

study on threats to information network operations. The Cyber Command study defines insider threat as:

> The "insider" is anyone who is or has been authorized access to a DOD information system, whether a military member, a DOD civilian employee, or employee of another Federal agency or the private sector. Some recommendations, however, address the broader scope of "system components" or "computer software code" inside a system and intended to carry out a malicious act.[10]

The U.S. Army uses the military intelligence community definition, which depicts a slightly different threat than Cyber Command. The definition within the scope of counter-intelligence investigations is defined as:

> A person with placement and access who intentionally causes loss or degradation of resources or capabilities or compromises the ability of an organization to accomplish its mission through espionage, providing support to international terrorism, or the unauthorized release or disclosure of information about the plans and intentions of U.S. military forces.[11]

Although the U.S. Army identifies and defines insider threats, it is only in the military intelligence community that it ties insider threats to terrorism. This connection is only tied to international terrorism. The connection is appropriate for a counter-intelligence officer that is restricted in investigations, but it does not facilitate an investigation on anyone that does not have ties outside the U.S. A U.S. Army leader that has an insider threat in their organization, which is a homegrown terrorist, may not necessarily be tied to organized international terrorist effort. Instead, the leader may be a

---

[10]Department of Defense, *DOD Insider Threat Mitigation* (Falls Church, VA: Information Assurance Technology Analysis Center, n.d.), i.

[11]U.S. Army Military Intelligence, Army Regulation 381-12, *Threat Awareness and Reporting Program* (Washington DC: Government Printing Office, 4 October 2010), 4.

sole actor and also known as a lone wolf terrorist. Further research determined the US Army does not operationally define the insider threat term for a leader's use. This term does not have adequate characteristics assigned to identify it or actions required if a threat is identified. Insider threat terms do not exist in the U.S. Army's command policy, nor is there a separate definition for insider threat in U.S. Army leadership manuals.[12]

This problem of defining the threat is larger than U.S. Army intelligence and network system security, President Barrack Obama approved Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and Responsible Sharing and Safeguarding of Classified Information*.[13] This order established the Department of Defense (DOD) in conjunction with the National Security Agency (NSA) as the lead executive agents for safeguarding information.[14] Each department is responsible for establishing their own insider threat program while the Presidential Order mandates the requirement for a federal insider threat program.[15] The order also directs the establishment of the Federal Insider Threat Task Force to facilitate the proposals in the

[12]Headquarters, Department of the Army, Army Regulation 600-20, *Army Command Policy* (Washington, DC: Government Printing Office, 4 August 2011); Headquarters, Department of the Army, Field Manual 6-22, *Army Leadership Competent, Confident, and Agile* (Washington, DC: Government Printing Office, 12 October 2006).

[13]White House, Executive Order 13587 Structural reforms to improve the Security of Classified Networks and Responsible Sharing and Safeguarding of Classified Information, http://www.whitehouse.gov/the-press-office/2011/10/07/executive-order-13587-structural-reforms-improve-security-classified-net

[14]Ibid.

[15]Ibid.

federal insider program.[16] The task force is co-chaired by the Attorney General and the Director of National Intelligence with members from all the other U.S. Federal Executive Departments and CIA.[17]

Following the Fort Hood shooting and before the executive order there were a number of inquiries and reports, many of which have been reviewed in Congressional testimony. Paul Stockton, the Assistant Secretary of Defense (ASD) for Homeland Defense and America's Security Affairs (HD & ASA) testified before the Homeland Security Committee on 7 December 2011. During his testimony Stockton stated that:[18]

> There is an effort within the Insider Threat Working Group to "establish a single, DOD-wide definition of insider threat as "A person with authorized access, who uses that access, wittingly or unwittingly, to harm national security interests or national security through unauthorized disclosure, data modification, espionage, terrorism, or kinetic actions resulting in personal injury or loss or degradation of resources or capabilities." Under this broad strategic umbrella, individual DOD components may initiate programs tailored to address their distinctive vulnerabilities.[19]

Assistant Secretary Stockton testified there is a need to broaden the scope of the insider threat definition. While the Insider Threat Task Force works on a federal insider threat

---

[16]Ibid.

[17]Ibid.

[18]The Insider Threat Working Group is the working group that reports to the DOD Force Protection Steering Committee led by the Assistant Secretary of Defense for Homeland Defense and America's Security Affairs, Paul Stockton. This Group was established to synchronize efforts and changes across all DOD following the Fort Hood Shooting and the wiki leaks scandal in order to establish a DOD insider threat program.

[19]Assistant Secretary of Defense for Homeland Defense and America's Security Affairs Paul Stockton speaking before the Committee on Homeland Security and the Senate Committee on Homeland Security and Governmental Affairs. *Homegrown Terrorism: The Threat to Military Communities Inside the United States,*112th Congress, 7 December 2011.

program, the DOD is widening the aperture of its insider threat definition and so must the U.S. Army. Properly broadening the definition guarantees it is viewed as a larger leadership issue, ensuring the U.S. Army does not marginalize the topic as just an information security or military intelligence issue.

For the purpose of this thesis, the drafted Insider Threat Working Group definition of insider threat is used. The insider threat working group definition is the broadest definition acknowledging that an insider threat is someone that wishes to cause harm and destruction to the United States through various means. This definition is not limited to the insider working with another country or actor. Additionally, for the purposes of this paper the definition for radicalized behavior or radicalization will refer to "departing markedly from the usual; extreme also to advocate fundamental or revolutionary changes."[20]

Identifying Insider Threat

Since the Federal Government and DOD are still uncovering a standard definition, they have not clearly outlined the characteristics for identifying an insider threat. This study will address the challenges faced by the U.S. Army to identify these threats, and recommend actions to counter it. Although insider threat incorporates a large scope of threats, this thesis will address the menace of homegrown terrorists and radicalized individuals as threats to the U.S. Army.

[20]Margery S. Berube, et. al., *American Heritage Dictionary* (New York: Dell Publishing, 1992), 680.

There is a great deal of research on insider threat throughout the U.S. private sector; however, the majority of the research views the issue as a communications network systems issue. Often the homegrown terrorist is seen as a separate issue, and there is often a lack of awareness to correlate the two problems under the insider threat umbrella. Follow-up procedures for leaders to take after identification are seldom outlined, and there is a critical lack of a recommended timeline in which a leader should take action using these resources.

U.S. Army leaders are responsible for the failures and successes of their personnel. It is critical that a process exists that helps them to identify and address insider threats so leaders can act appropriately and in a timely manner. This process is vital because leaders may be faced with determining the difference between a high risk Soldier that presents a threat to the good order and discipline to the unit and a Soldier who exhibits radicalized beliefs and could pose a serious force protection threat to the unit. Therefore, the process of recognizing the threat must acknowledge and define the differences, in order for it to be a successful tool for leaders.

Although Army leadership is responsible for implementing the internal vetting required by the Army, ultimately the Federal Insider Threat Task Force must synchronize and manage a plan to keep Americans safe from the homegrown terrorist threat. Although the Federal Government must develop the strategy, the U.S. Army must be more capable in defending itself from these threats.

When investigating solutions to the problem of identification, it is important to look at other, similar examples of vetting procedures currently utilized in other U.S. organizations. Understanding current procedures, internal and external to the U.S. Army,

and then comparing these procedures against the Fort Hood shooting incident is a way to identify the criteria that is necessary to properly identify insider threats.

Assumptions

In order to compare the programs, there are several assumptions that must be made for research to proceed. First, there is an assumption that the insider threat of radicalized individuals is a growing issue, which the Army must mitigate. It is also assumed that the Fort Hood shooting is a valid example of an insider threat in order to facilitate a comparison of different insider threat processes.

Scope and Limitations

Scope

This thesis relies on resources outside the U.S. Army due to the relatively recent nature of depicting the insider threat within the U.S. Army, and there is a paucity of military research and writing on the topic. In order to understand the definition and parameters that combine the homegrown terrorism threat with the insider threat, the thesis will conduct a document study on the Fort Hood shooting to use and apply the lessons learned in comparison to the Army's recommended processes.

The Fort Hood shooting case is used as an example for illustrating the insider threat and revealing criteria that differentiate this threat from the threat of other high risk individuals. The presumption is there is a process that leaders can follow to identify all threats to the organization, and then clearly differentiate between high risk individuals and those that pose insider threats to cause harm to the U.S. Army.

This study will conduct a qualitative analysis of the recommended process for identifying insider threats in comparison to criteria determined necessary by the Fort Hood shooting example. An example of one of the recommended processes is the U.S. Army's Force Protection Level I training found in Army Regulation 350-1.[21] In addition to insider threat identification model comparisons, this thesis will determine and seek recommendations for training that can be taught to U.S. Army leaders at all echelons to help them identify insider threats.

Limitations

The study is limited to unclassified material, in order to maintain the ability to share processes that identify insider threats that can be openly disseminated. This study is limited to the analysis and application of the Fort Hood shooting as the identified example. The limiting of this study is due to time restraints, and the necessity to focus on homegrown terrorism and radicalized individuals under the insider threat umbrella. This thesis is also limited to lessons learned within the United States.

Furthermore, this study is not conducted to form an opinion or determine the leadership's appropriate conduct and response to Major Nidal Hasan's behavior and actions before the event. Nor is this study to make a determination of blame for the responsibility of the Fort Hood shooting or any other insider threat, but rather to discover trends and lessons to apply to the process of identifying insider threats.

[21]The U.S. Army's Regulation 350-1 4 August 2011, outlines mandatory yearly training. Force protection Level One training is outlined as an annual requirement for all individuals serving in the U.S. Army.

Delimitations

This study is limited to the Fort Hood shooting case; however, the data is further limited as Major Nidal Hasan is still pending trial. There is limited unclassified research and reviews of other cases of insider threats, but this could be an area for follow-on research as more information becomes available.

CHAPTER 2

LITERATURE REVIEW

The Insider Threat Task Force established by the President is responsible for synchronizing and guiding the comprehensive federal program on insider threat. While the task force conducts this development and synchronization, the U.S. Army is also moving forward in working to prevent insider threats. There are a significant number of lessons that can be learned from the Fort Hood shooting case, as an insider threat that garnered significant negative publicity and was seriously detrimental to the U.S. Army and its image.

One of the most significant lessons learned is the pivotal role of leaders in the identification process. Several articles and reviews cite the leadership failures of Major Hasan's superiors. This study investigates whether the U.S. Army has instituted sufficient processes to train leaders to distinguish these threats. This literature review will delve into the U.S. Army's insider threat and the ability to identify the homegrown terrorist.

Research Questions

To help prevent an incident similar to the Fort Hood shooting, this study seeks to answer: whether U.S. Army insider threat identification procedures enable leaders to determine a homegrown insider threat like the threat of the Fort Hood shooting.

Before this study can answer the research question, the literature review must validate its assumptions. The first assumption is that radicalized, insider threat individuals are a growing issue, which the U.S. Army must mitigate. Another assumption

is that the Fort Hood shooting case is a valid example of this type of insider threat to use to compare the processes.

The research is divided into four areas of study. The first area of study determines the parameters of the homegrown terrorist insider threat. Reviewing the U.S. Army's insider threat will validate the first assumption that this topic is a real issue, and that there is a necessity to deter the threat further.

The second area of focused research is on the Fort Hood shooting. This discovery intends to confirm that the Fort Hood shooting is a relevant example of insider threat to the U.S. Army. By understanding this example, improved characteristics can be applied when evaluating models.

The third area of focus is the examination of current practices and trends for identifying insider threats within the United States private sector. With an understanding of experts' recommended modeling, the three assumptions can be analyzed and validated for evaluation criteria for the U.S. Army's identification processes.

Lastly, the literature review summarizes three models of detection for insider threats that are promoted within the U.S. Army, but are not taught as a U.S. Army leader identification model for insider threats. This set of reviews determines what types of models the Army already possesses for identifying the threat.

Determining the Insider Threat

The Obama Administration recognized the significance of the homegrown threat in the June 2011 National Strategy for Counter-terrorism.[22] In November 2011, Jerome P. Bjelopera published a Congressional Research Service report titled *On American Jihadist Terrorism*. Jerome P. Bjelopera, a member of the Congressional Research Service, is a part of a component that concentrates on crime and terrorism. His report cited fifty-three homegrown terrorist plots involving hundreds of suspects since 11 September 2001.[23]

> From May 2009 through October 2011, arrests were made for 32 "homegrown" . . . terrorist plots by American citizens or legal permanent residents of the United States. Two of these resulted in attacks—U.S. Army Major Nidal Hasan's alleged assault at Fort Hood in Texas and Abdul Hakim Mohammed's shooting at the U.S. Army-Navy Career Center in Little Rock, AR—and produced 14 deaths.[24]

This report revealed there has been a spike in attacks. Between 2009 and 2011, there have been more attacks in two years then in the seven years following 11 September 2001.[25] It was also determined that lone wolf or sole actors have been the most successful at conducting insider threat attacks. Major Hasan is considered a successful lone wolf actor, according to Bjelopera's report. Major Hasan is accused of

---

[22]The White House, *National Strategy for Counterterrorism*, June 2011, http://www. whitehouse.gov/sites/default/files/counterterrorism_strategy.pdf (accessed 24 February 2012).

[23]Jerome P. Bjelopera, *American Jihadist Terrorism: Combating a Complex Threat* (Washington, DC: Congressional Research Service, 15 November 2011), 1.

[24]Ibid., Summary.

[25]Ibid.

perpetrating the actions at the Fort Hood shooting on his own, without coercion or sophisticated planning.

The report asserts an individual that expresses radicalized views should be watched for the potential of becoming a homegrown terrorist.[26] When that person begins to take actions based on radicalized views, they should be considered a terrorist at that time as well as an insider threat.[27] Bjelopera also asserts that as people transition to terrorist, they often express and develop their radicalized views through social networking and Internet sites.[28] Thus, there is an expectation that an insider could be monitored through an information system security.

Bjelopera reports that an Al Qaeda media release in 2011 encouraged more attacks like the one at Fort Hood.[29] There is a compelling challenge to deter insider threats as Al Qaeda's media release urges more individual terrorist actions, which promotes an increased chance of lone wolf attacks.

The Homegrown Terrorism Threat to the Military

According to the New America Foundation and Syracuse University Maxwell School, there have been 192 personnel from the United States who have participated in homegrown plots and activities directed at the United States as acts of terrorism since

[26]Ibid., 41.

[27]Ibid., 2.

[28]Ibid.

[29]Ibid., 9.

2001.[30] All 192 individuals have had formal allegations of breaking laws pertaining to their conduct or intentions of attacking American personnel within the U.S. and abroad.[31] The Fort Hood shooting case is listed as one these cases and as an example of homegrown terrorism.

Of the 192 terrorist cases in America, the Foundation determined there were sixty-six cases that involved a U.S. military target. These targets were either military personnel or military installations. Of the cases, thirty-six were U.S. targets abroad, and thirty were targets within America. The majority of these cases were incidents involving a suspect who was determined to be a homegrown terrorist. The report states, "Around one in three of such cases involved a U.S. military target."[32] The greater percentage of the U.S. military presence overseas is comprised of U.S. Army personnel followed by the U.S. Air Force.[33] Therefore, as long as America's military remains a target then the U.S. Army will remain a target.

High Risk Individuals at the Expense of Manning the Force?

The Army has been consistently deployed in conflict over a decade, increasing the need to grow and maintain the force. In an effort to remain an all-volunteer force, the U.S. Army increased the waiver and retention of subpar Soldiers to meet its wartime

---

[30]New America Foundation and Syracuse University's Maxwell School.

[31]Ibid.

[32]Ibid.

[33]Office of the Deputy Under Secretary of Defense for Instillations and Environment, *FY 2011 Base Structure Report* (Washington, DC: Government Printing Office, 2011), 25.

needs.[34] As the Army's deployments decrease, there is a push from senior leaders within the U.S. Army to train staffs and leaders to better identify high risk Soldiers.[35]

Two media sources indicate that the U.S. Army's emphasis to retain sufficient personnel to fight external threats may have been at the expense of the Army. Retention concerns and the potential fear of being labeled anti-Muslim, encouraged ignoring indicators that increased the liklihood of the shooting. The Fort Hood shooting is an example of a high risk individual that was overlooked for U.S. Army manning requirements. The Pittsburg Post Gazette referred to Major Hasan as a high risk individual, and suggested the Army's acceptance of high risk individuals may have been a factor in Hasan's retention.

> According to information gathered during the internal Pentagon review . . . Mr. Hasan's strident views on Islam became more pronounced as his training progressed. Worries about his competence also grew, yet his superiors continued to give him positive performance evaluations that kept him moving through the ranks.[36]

Although Major Hasan was seen as a high risk individual, he was allowed to progress in the U.S. Army. Individuals can exhibit high risk behaviors and be an insider threat simultaneously. Consequently, it is essential that all personnel recognize high risk behavior, while understanding the characteristics that tie this behavior to homegrown terrorism.

---

[34]Michelle Tan, "Tougher Discipline as Optempo Eases," *The Army Times*, 3 July 2011, http://www.armytimes.com/news/2011/07/army-tougher-discipline-enforced-070311w (accessed 10 March 2012).

[35]Ibid.

[36]*Pittsburgh Post-Gazette*, "Ft. Hood Officers Face Punishment," 15 January 2010, http://www.proquest.com.lumen.cgsccarl.com/ (accessed 25 February 2012).

What Can Be Learned From the Fort Hood Shooting?

Bjelopera and the Maxwell School both classify the Fort Hood shooting as a terrorist threat. Since Al Qaeda has endorsed the Fort Hood shooting as an example to emulate, there must be an enquiry into Major Hasan's behavior. Analysis of reports aid in providing insight and understanding of the events prior to the shooting to better recognize patterns of insider threats.

Currently, Major Hasan "is charged with thirteen counts of pre-meditated murder and thirty-two counts of attempted murder."[37] His court-martial is currently scheduled for 12 June 2012. Therefore, the literature review will be compiled from unclassified media sources such as *National Public Radio*, *Time Magazine*, the *Associated Press*, and the testimony of Senator Joseph I. Lieberman in lieu of trial records.

Nidal Malik Hasan was an active duty Army officer serving at Fort Hood, Texas in the capacity of a psychiatrist. He is charged with entering the Fort Hood Deployment Readiness Center, shooting and killing thirteen individuals most of whom were a part of his medical staff, and wounding thirty-two more on 5 November 2009. Major Scott Moran is one of the personnel who oversaw Captain Hasan's actions in the residency program and documented his concerns regarding Hasan. *National Public Radio* (NPR) reported in 2009 that Major Scott Moran had characterized Major Hasan's performance while serving at Walter Reed Army Hospital as, "an incompetent psychiatrist and an

[37]Phillip Jankowski, "Judge delays Hasan court-martial until June," *Killeen Daily Herald*, 2 February 2012, http://www.kdhnews.com/news/story.aspx?s=63990 (accessed 12 February 2012).

unprofessional officer who often neglected his duties and his patients."[38] Moran's concerns regarding Hasan are evidenced in all four resources. It is in the *Time* magazine article that he states the leadership concerns about Major Hasan in 2008 led to a meeting of several leaders and staff at Walter Reed Hospital to discuss then Captain Hasan's work performance.[39] In spite of the meeting and leadership concerns, Hasan continued to progress and serve in the U.S. Army.

In a review of Major Hasan's evaluations, none of his leaders documented the negative performance noted by Major Scott Moran.[40] Further research uncovered that Major Hasan held radical views on Islam, which were prevalent throughout his time at Walter Reed Army Medical Hospital.

> Evidence of Hasan's radicalization to violent Islamist extremism was on full display to his superiors and colleagues during his military medical training. An instructor and a colleague each referred to Hasan as a "ticking time bomb." Not only was no action taken to discipline or discharge him, but also his Officer Evaluation Reports sanitized his obsession with violent Islamist extremism into praiseworthy research on counterterrorism.[41]

In a memorandum, Major Hasan's conduct and obsession with radical Islam was not only noted by his superiors, but he was also reported to have a poor work ethic as a

---

[38]Daniel Zwerdling, "Evaluation Raised Concerns About Maj. Hasan in '07," NPR.com, 19 November 2009, http://www.wbur.org/npr/120562890/evaluation-raised-concerns-about-maj-hasan-in-07 (accessed 2 May 2012).

[39]Nancy Gibbs, "Terrified or Terrorist?" *Time Magazine,* 23 November 2009, 30.

[40]*Pittsburgh Post-Gazette,* "Ft. Hood Officers Face Punishment," 15January 2010, http://www.proquest.com.lumen.cgsccarl.com/ (accessed 25 February 2012).

[41]Senate Committee on Homeland Security and Governmental Affairs, "A Ticking Time Bomb: Counterterrorism Lessons from the U.S. Government's Failure to Prevent the Fort Hood Attack." 112th Congress, 1st Sess. (15 February 2011). http://www.hsgac.senate.gov/ (accessed 12 April 2012), 8

captain in the U.S. Army.[42] The failure to report his Islamic extremist activities and to overlook his poor work allowed Hasan to be promoted from captain to major. Further reports by *National Public Radio* indicated that a memo "shows that Hasan proselytized to patients. He mishandled a homicidal patient. He allowed her to escape from the emergency room [and] when Hasan was supposed to be on call for emergencies; he did not even answer the phone."[43]

An interview of Major Hasan's Walter Reed classmate in a Time Magazine article indicates there were several incidents that highlighted Hasan's radical beliefs. Hasan chose to conduct a briefing entitled, "War on Terror was a War on Islam" when he was to brief a subject that related to public health.[44] Additionally, Hasan's classmate discussed that Hasan frequently spoke of how he favored Shari'a law, and his identity as a Muslim above that of an Army Officer and the defense of the Constitution.[45] As one can see, there were a number of high risk indicators that should have warned his superiors. Ultimately, Major Hasan's noted radicalization displayed insider threat characteristics that should have been reported and acted upon.

---

[42]Daniel Zwerdling, "Hasan's Supervisor Warned Army in 2007," NPR.org, 18 November 2009, http://www.npr.org/templates/story/story.php?storyId=120540125 (accessed 14 April 2012).

[43]Ibid.

[44]Nancy Gibbs, 29.

[45]Ibid., 29.

Testimony from Senator Joseph Lieberman on
His Report of the Fort Hood Shooting

Senators Joseph I. Lieberman and Susan M. Collins, Republican from Maine and Ranking Senate Committee Member for the Committee on Homeland Security and Governmental Affairs, compiled a report entitled, "A Ticking Time Bomb," and presented it to the Homeland Security and Governmental Affairs Committee on 11 February 2011. Senator Lieberman's testimony is relevant because he cites leadership failures and the failures of a multitude of people to recognize the radicalized insider threat.

Senator Lieberman stated in his presentation that the U.S. Army failed to discipline Major Hasan, and instead promoted him and viewed his radical ideas as virtuous, dismissing them as research.[46] Additionally, Senator Lieberman noted numerous governmental failures. First, he stated that the Federal Bureau of Investigations failed to act on reports about Major Hasan, instead concluding that the doctor was doing research.[47] Leiberman also stated the U.S. Army does not recognize or define violent Islamic extremism within Army policy documents.[48] The most pronounced conclusion that resonates throughout this paper is Senator Lieberman's ascertainment that there is "a troubling lack of awareness among some government officials about violent Islamist

[46]Senator Joseph I.Lieberman, Senator Susan A. Collins, Charles E. Allen, and John M. Keane, "A Ticking Time Bomb: Counterterrorism Lessons from the U.S. Governments Failure to Prevent the Fort hood Attack," Homeland Security Digital Library, www.hsdl.org/?view&did=7760 (accessed 6 April 2012), 29-30.

[47]Ibid., 30.

[48]Ibid.

extremism, the ideology that inspires it, its signs and manifestations, and how to confront it."[49] The government as a whole does not understand the threat posed by violent extremists or radicalized individuals.

Officership Training Evaluation of the Army Medical Department Center and School

In response to Senator Lieberman's report, the Department of Army directed the Army Medical Command in March of 2011 to conduct a review of their leadership training. The Leader Training Center in MEDCOM completed this review and their report was published May 2011.

The committee members conducted a review of MEDCOM systems, policies, and procedures. They concluded:

> As a result of investigations following the Fort Hood shooting, the Secretary of the Army directed the CG MEDCOM to review MEDCOM policies and procedures for (1) drafting evaluations, (2) ensuring compliance with Army physical fitness and height/weight/body fat standards, and (3) counseling and flagging Soldiers involved in medical training and education programs, and to examine whether the training curriculum for new Army medical officers should place additional focus on officership.[50]

The report gleaned from Congressional testimony that there is a leadership problem, concluding that medical officers must adjust entry medical officer education to coincide with other U.S. Army officer education, such as the U.S. Army's Basic Officer Leader Course. The report also added required focus on leadership counseling.

---

[49]Ibid., 29.

[50]Colonel Carl C. Bolton, MAJ Soraya Turner, MAJ William Ritter, and Hank Sebastian, *Officership Training Evaluation of the Army Medical Department Center and School* (San Antonio, TX: Leader Training Center, 2011), 7.

Although the report determines that there are weaknesses in the broader leadership training of medical officers, it does not mention a need to train officers or leaders on the topic of radicalized views, homegrown terrorism, or insider threat recognition. The report neither mentions a need to increase emphasis on MEDCOM's anti-terrorism training, or threat awareness training, nor does the report identify the need to train leaders to identify or place emphasis on identification of high risk individuals or any form of insider threats.

The Army Acknowledges Insider Threat is an Army Leadership Issue

The U.S. Army's Insider Threat Task Force was established at Fort Meade, Maryland in 2010 following the published findings from the Department of Army's review of the Fort Hood shooting. A member of this task force, discussed the complexity of identifying an insider threat in an interview in the INSCOM Journal.

> The best example I can give is workplace violence, he said. "You hear about some guy going "postal" and killing 13 people. The next thing you know, everyone is blaming the police for not stopping it. But how could the police have known that this guy could have done this? There are people in his office who probably saw signs and could have spoken up to prevent it."[51]

The member of the task force stated that the Army and its leaders must be educated on the threat in order to identify the warning signs. If leaders understand the warning signs, they can address the issues and mitigate the threat.[52] Not only is there a need for

[51]Brian Murphy, "Everything Changed," *INSCOM Journal* (Summer 2010), http://www.inscom.army.mil/journal/2010/summer10/10summer2.html (accessed 6 April 2012).

[52]Ibid.

education to identify insider threats before they act or when they reach out, but there must be an understanding of when to report unfavorable behavior and to which agency to report.

Findings from U.S. Army Reports on the Fort Hood Shooting Conclude the Army Must Train Their Leaders

Bill Gertz, a national security columnist for the *Washington Times* and an author of six national security books, reported in the *Washington Times* on the *Fort Hood Army Internal Report* that the Army released in 2010. Gertz stated the report indicated the Army's immediate response to the 5 November 2009 incident was effective; however, there was not sufficient evidence on the DOD's preparedness procedures to indicate if they could have prevented the incident.[53] Gertz continued to summarize in the report that U.S. military policies do not identify "indicators of violence," and those military policies that do exist "are outdated, incomplete and fail to include key indicators of potentially violent behaviors."[54]

Although Major Hasan has not yet stood trial, there have been a number of reports and studies related to the case to determine where improvements can be made to prevent future incidents of this nature. The *Fort Hood Army Internal Report* recommends the need to train and develop more in-depth installation checks and personnel screening

[53]Bill Gertz. "Report: Army failed to identify Fort Hood threat," *Washington Times*, 10 November 2010, http://www.washingtontimes.com/news/2010/nov/9/report-army-failed-to-identify-fort-hood-threat/?page=all (accessed 6 April 2012).

[54]Ibid. Gertz also reported that Senator Lieberman criticized the inquiries and reporting for not citing the Fort Hood incident as a terrorist attack.

procedures to identify internal threats.[55] In addition to the Army's report, the DOD report recommends sharing of information across services as well as the updating of policies.[56]Besides the sharing of information, DOD recommends the Defense Science Board conduct a study in the determination of the characteristics of violent radicalization.[57] The Air Force, too, concluded, in the *Air Force Follow-On Review: Protecting the Force* that the focus should not be so much on external threats as internal threats as they are the more serious issue.[58] The process of educating leaders is essential in preventing attacks from this threat.

Identifying the Insider Threat

There are multiple methods to identify an insider threat. The majority of currently studied and published reports, recommendations, and methods view insider threats as a communications network security issue. On the other hand, the bulk of terrorist and threat research indicates that the approach to fixing this problem needs to address both the radicalized extremist and education issues. This portion of the literature review analyzes

[55]Department of the Army, *Fort Hood Army Internal Review Team Final Report: Protecting Our Army Community At Home and Abroad* (Washington, DC: Fort Hood Army Internal Review Team, 4 April 2010).

[56]Department of Defense, *Protecting the Force: Lessons from Fort Hood: Recommendations of sharing information across services* (Washington, DC: U.S. Department of Defense, 2010).

[57]Ibid.

[58]Chris Cain, *Air Force Follow-On Review Protecting the Force, Lessons From Fort Hood* (Washington, DC: Dept. of the Air Force, 2010).

the work that has been conducted to identify the insider threat and model it as it pertains to radicalized individuals.

American Radicalized Threat

Jerome P. Bjelopera, an author who specializes in organized crime and terrorism, published a *Congressional Research Service Report* on American jihadist terrorism. His work highlights the complexity of identifying the point at which someone who is considered to have radical beliefs turns to violence.[59] The report determined that not all radicalized individuals go through a systematic process to become violent, therefore, making a linear progression hard to conclude.[60]

This report discusses the difficulty in determining when a homegrown terrorist, particularly a lone wolf actor, becomes a threat. Their interests are evident only in their radicalized beliefs, and their action against a target is often conducted without training, is ill-prepared and unsophisticated.[61] Bjelopera's report describes MAJ Hasan as an example of a radicalized threat, pointing to Major Hasan's correspondence of sixteen emails with Anwar Al-Awlaki, a radical Imam accused of recruiting for Al Qaeda.[62] Several times he cites how terrorists utilize social networking and the Internet as means

---

[59]Jerome P. Bjelopera, *American Jihadist Terrorism: Combating a Complex Threat* (Washington, DC: Congressional Research Service, 15 November 2011).

[60]Ibid., 2.

[61]Ibid.

[62]Ibid., 92.

of retrieving information.[63] Bjelopera recommends that Congress conduct oversight on the Executive Branch's countering violent extremists policy. He infers that the policy is not comprehensive in implementing programs for this complex, homeland threat.[64]

Beljapera refers to the President's *Strategy on Empowering Local Partners in Preventing Violent Extremism in the United State*s, which was issued in August of 2011 as the national direction to countering violent extremism.[65] A month after Beljapera's report, the President issued his corresponding *Strategic Implementation Plan on Empowering Local Partners in Preventing Violent Extremism in the United States* in December of 2011.[66] This plan outlines more specifics for programs to include lead departments and future actions. For example, the Department of Homeland Security has the lead in developing training and programs with local law enforcement and local communities to counter violent extremism particularly digital forums for training and sharing of lessons learned. Moreover, this plan outlines the necessity of the DOD Force Protection Steering committee that was established in response to the Fort Hood follow on review.[67] The plan also projects five future activities for the DHS, FBI, National

---

[63]Ibid., 14-19.

[64]Ibid., 68.

[65]The U.S. President, *Strategy on Empowering Local Partners in Preventing Violent Extremism in the United States* (Washington, DC: Government Printing Office, August 2011).

[66]The U.S. President, *Strategic Implementation Plan on Empowering Local Partners in Preventing Violent Extremism in the United States* (Washington, DC: Government Printing Office, December 2011), 1-12.

[67]Ibid., 13.

Counter Terrorism Center and the State Department to develop. Three of these future endeavors are to expand the study of radicalization and the internet, lone wolf terrorists, and indicators of extremist violence.[68]

Applying a Multiple Echelon Approach to Identifying Insider Threats

There are few reports that discuss an insider threat as a radicalized individual. One author that does is Nick Catrantzos. Catrantzos is a graduate of the Naval Post Graduate program in Homeland Studies and is considered an expert in a range of homeland security and national defense topics. He identified a number of issues associated with detecting insider threats. The American Society for Industrial Security International Foundation (ASIS), whose focus is on researching new and emerging security measures and threats, sponsored a report written by Catrantzos, *Tackling the Insider Threat*. This report advocates and identifies the linkage of the insider threat across different mediums, such as workplace violence and espionage.[69] Catrantzos advises the use of multiple layers of detection by institutions for an in-depth defense.[70]

Catrantzos referenced previous research in his Master's thesis for the Center for Homeland Defense and Security and the Naval Postgraduate School.[71] His Master's thesis pointed out that protection measures intended for security of critical infrastructure

---

[68]Ibid., 14.

[69]Nick Catrantzos, *Tackling the Insider Threat* (Alexandria, VA: ASIS Foundation, 2010), 5.

[70]Ibid.

[71]Ibid., 17.

would not deter insider threats. His work validated the fact that a perpetrator acting as a significant, critical insider threat would already know the internal security measures of an institution, for instance the Army's force protection measures. Therefore, a true internal threat could neutralize those protective measures. His research determined the most likely person to conduct a terrorist attack or try to cause severe harm to an institution would be someone who was already established within the organization, and had an understanding of how to circumvent security measures.[72] His research further indicated that someone who conducts a terroristic or critical insider attack is neither new to the institution nor a disgruntled employee; rather the attacker is most likely to conduct an attack based on divergent ideology.[73]

The Reason Network Security Works for Identifying Insider Threats

Divergent ideology is a significant indicator for identifying a radicalized individual ideology that could trigger the onset and the development of a homegrown terrorist and by extension an insider threat. There is a need to monitor and determine this type of threat. The monitoring of individual's correspondence over the Internet is one of the most proactive methods that law enforcement and the FBI utilize to obtain information about possible terrorist activities in the United States.[74] Law enforcement

[72]Ibid., 16-17.

[73]Ibid

[74]Bjelopera, "American Jihadist Terrorism," 3.

agents and the FBI have gone undercover on social websites to monitor correspondence of suspected terrorists and criminals.[75]

In order to reduce the vulnerabilities caused by insider threats to the Army, there must be a concerted effort to establish linkages of the threats across different mediums like social websites, network security, and training. The FBI is just one source for detecting insider threats. There are many other methods to detect insider threats: one medium is an information system; however, these threats are also indicated in several mediums such as workplace violence, corporate security, and espionage.[76] Therefore, the detection should be across several systems in order to correlate identification measures.

Whitepaper on Simulation Information to Insider Threat Detection

Dr. Eric A. Cole, an expert in cyber security, authored a white paper on correlating simulation (SIM) information to insider threat detection. Dr. Cole makes recommendations for a threat profile by correlating data from corporate insider threat studies conducted by the U.S. Secret Service and the Computer Emergency Response Team (CERT).[77] Dr. Cole indicated, through analysis of the data he had compiled in Table 1, "that the insider's primary goal was to sabotage an aspect of the organization."[78]

---

[75]Ibid., 3.

[76]Catrantzos.

[77]CERT is a registered trademark to the Carnegie Mellon University that directs the Software Engineering Institute, they focus on Cyber Security threats and responses and are primarily funded by DOD and DHS.

[78]Dr. Eric A. Cole, SANS Whitepaper, "Correlating SIM information to Detect Insider Threats," 5.

Table 1. Profiling an Inside Attacker According to SANS White paper Results
80% of insiders who launched attacks on their companies had exhibited negative behaviors before the incident
92% had experienced a negative work-related event, such as a demotion, transfer, warning, or termination
59% were former employees or contractors (48% had been fired, 38% had resigned, 7% had been laid off)
41% were still employees
86% were employed in a technical position (38% of them were system administrators, 21% were programmers, 14% were engineers,14% were IT specialists)

Source: Dr. Eric A. Cole, *Correlating SIM information to Detect Insider Threats* (SANS Whitepaper), 5.

Dr. Cole's analyses of CERT and Secret Service data determined that profiled insiders often display warning signs. These warning signs can often be seen in the company's SIM system. "A SIM system can seamlessly take the information from many different networking and application logs, correlate that information, aggregate patterns, and produce focus areas to use to detect an insider causing harm" to the company.[79] Dr. Cole recommends to first establish a baseline from which to analyze the network so the employer or supervisor can determine an employee's degradation in behavior.[80] After establishing a baseline, the SIM can monitor differences in the inbound and outbound Internet traffic, including the amount of data and the most active time periods employees conduct their correspondence.[81] As a result, an employer can compile a comprehensive

[79]Cole, 3.

[80]Ibid., 8.

[81]Ibid., 11.

pattern of behavior and from that, develop an understanding of the questionable behavior that may be outside the norm.

The Layered Approach of Identifying Insider Threats Using a Scenario Based Approach

The layered approach of detection, such as the one Catrantzos describes, is discussed in *A Scenario Based Approach to Solving or Mitigating Threats*. The authors that developed this approach are Doctors of Philosophy with research in Network Security, and they served as associate professors at the Air Force Institute of Technology. Their scenario-based approach emphasizes analyzing insider threats in multiple layers starting with interactions with people, their processes, and use of technology to monitor information flow.[82] This process is depicted in Figure 1, which displays personal interactions or observables layered with informational auditing of cyber actions.

[82]Robert F. Mills, et al., "A Scenario-Based Approach to Mitigating the Insider Threat," *ISSA Journal* (May 2011): 12-19.

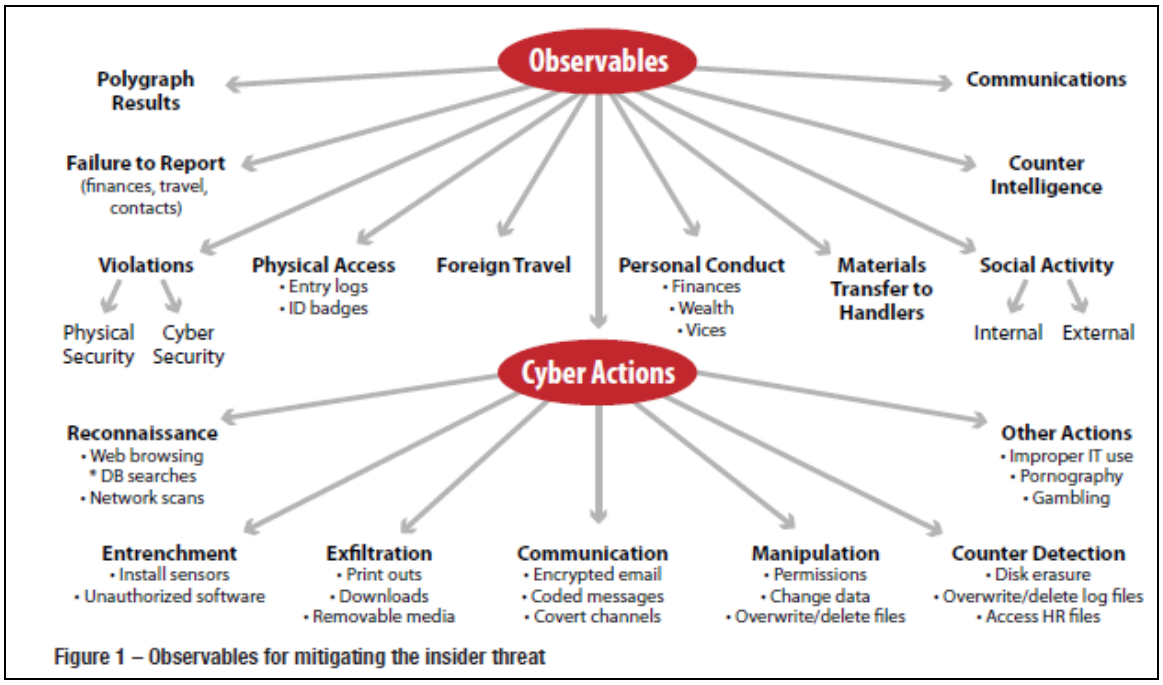

Figure 1 Model For Determining Insider Threat as Depicted in a Scenario-Based Approach to Mitigating the Insider Threat

Source: Robert F. Mills, et al., "A Scenario-Based Approach to Mitigating the Insider Threat," *ISSA Journal* (May 2011): 12-19.

The scenario-based approach discusses the ability of an organization to identify its critical information resources, and then works through scenarios with information from these resources, pinpointing possible insider attacks. Using this approach, the organization then conducts a simulation to determine the success of the systems and actions the organization has implemented. With this evaluation of systems, the organization can develop the necessary adjustments or validations for their in-depth defense systems.

Modeling Software to Detect Insider Threats

A similar model to the scenario-based approach is discussed in the application of situation-management modeling. In a situation-management modeling report presented at the International Conference on Information Fusion in September of 2008, there is a recommendation to build software for insider threat detection.[83] The ability to determine a person's intent is based on the ability to formulate a multitude of network events and transactions in modeling software and then conduct an audit function of insider threat identification.[84] This modeling software, coupled with behavioral indicators, is believed to provide multi-echelon detection. The application of modeling software is recommended based on increasing user transactions with outside and social networking applications. The application assists in determining intent and confirming insider threat behavior indicators. The model recommended by Buford is depicted in figure 2 and table 2.

[83]John S. Buford, "Insider threat detection using situation-aware MAS" (Keynote speech, 11th International Conference on Information Fusion, Cologne, Germany, 23 July 2008).

[84]Ibid.

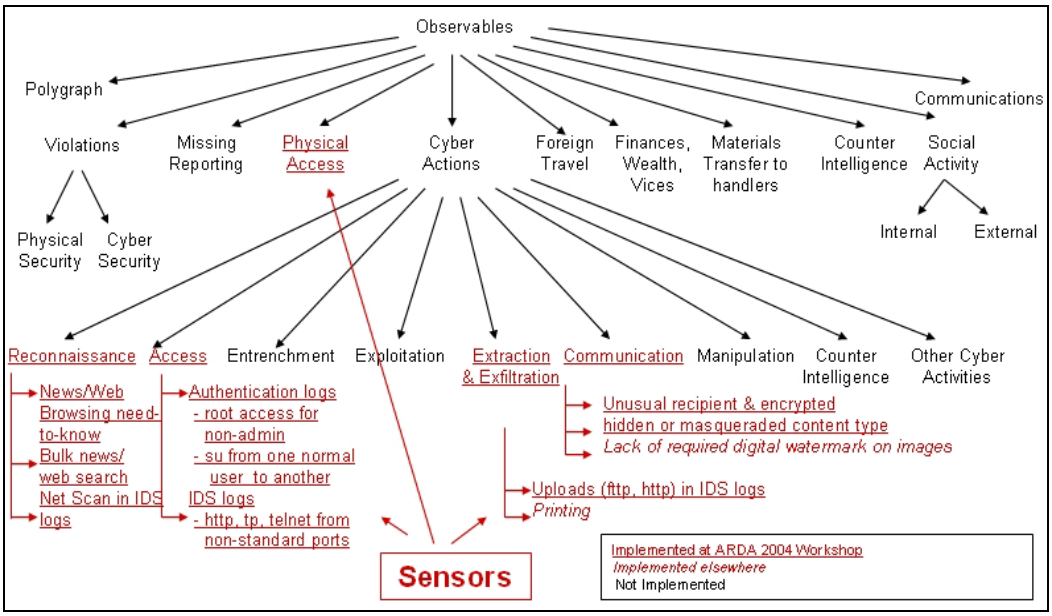

Figure 2 Insider Threat Detection Using Situation-Aware MAS.

Source: John S. Buford, Keynote speech, Information Fusion, 2008 11th International Conference on Information Fusion from FGAN, VDE, ITG, ISIF, Cologne, Germany, September 26, 2008.

Table 2. Insider Threat Detection Using Situation-Aware MAS Table.

Observable	Internal/External	Examples Captured Today Electronically
Polygraph	Internal	Human resource records
Violations	Internal	Human resource records
Missing reporting	Internal	Work flow records and other project reporting
Foreign travel	External	Credit card charges for foreign travel Credit card purchases while traveling Frequent flier and other traveler memberships Customs inspections Medical incidents occuring while traveling
Finances, wealth, vices	External	Motor vehicle violation in luxury car Online purchase and sale history Online auction history Side-business finances, bank accounts, and tax filings Personal tax returns and bank accounts Online gambling Casino preferred member programs
Material transfers to handlers	External	Personal computer use Call records on cell phones Unaccounted for absences
Counter intelligence	Internal	Evidence of intercepted communications and access to inside information
Social activity	Internal	Proximity as determined by computer use, id badge use, other location indicators in building
Social activity	External	Chat rooms, instant messaging, social networks, on-line games Proximity by location indicators such as cell phone or public WiFi network Position or auto GPS position Municipal surveillance
Communications	Internal & External	Call records

Source: John S. Buford, Keynote speech, Information Fusion, 2008 11th International Conference on Information Fusion from FGAN, VDE, ITG, ISIF, Cologne, Germany, September 26, 2008.

Defense Software Modeling

According to a recent news report in *Defense Systems*, the Defense Advanced Research Projects Agency (DARPA), in coordination with the Army Research Office, is preparing software that will detect insider threats.[85] The Anomaly Detection at Multiple Scales (ADAMS) program appears to implement a U.S. Army version of insider threat detection software. After first establishing an individual's baseline work habits, this software has an algorithm that detects abnormalities.[86] The intent is to implement network security monitoring and immediately build a baseline foundation to later detect anyone who conducts business outside the norm. The program is still in the testing phase, but it is forward movement for the Army in providing one level of in-depth defense against insider threats.

The U.S. Army's Identification Processes

The Army Anti-Terrorism Identification Recommendations

A significant portion of the U.S. Army's capability for in-depth defense, detecting, and recognizing insider threats requires training. The Army's Anti-Terrorism Force Protection (ATFP) training program has a model for identifying U.S. Army insider threats. The model cites examples like that of Fort Hood and the Wiki Leaks scandal as

[85]Henry Kenyon, "DARPA Seeks Early Detection of Insider Threats," *Defense Systems*, 17 November 2001, http://defensesystems.com/Articles/2011/11/17/DARPA-Anomaly-Detection-at-Multiple-S (accessed 14 March 2012).

[86]Ibid.

examples of insider threats to the U.S. Army.[87] The model cites eleven different insider threat characteristics to be aware of, and advocates only one layer of detecting these threats. The single layer of detection is an individual Soldier's responsibility; in essence every Soldier is a sensor. The ATFP insider threat detection model attempts to distinguish the difference between an insider threat and a high risk individual, as they chart mental instability in the training of insider threats.

Although the model covers several characteristics of the insider threat, it also groups a mentally unstable person with terrorists as an insider threat. Mentally unstable is defined as "persons that have a mental illness that impairs their judgment," and can exhibit many characteristics.[88] The characteristics for both a mentally unstable person and an insider threat are represented in Table 3, and ranges from references of suicide to a withdrawal from normal activities and relationships.[89] The behavior becomes insider threat specific when the subject commits an offense against the U.S. or when anti-American prejudices are observed.

[87]U.S. Army, "Identifying an Insider Threat" *Anti-Terrorism and Force Protection Level I Training*, https://atlevel1.dtic.mil/at/atl1/CONUS/insider/LevelC/insider_5/index.html (accessed 30 January 2012).

[88]Ibid.

[89]Ibid.

Table 3. Army's ATFP Level 1 Identification Model of Insider Threat

Source: U.S. Army, "Identifying an Insider Threat," *Anti-Terrorism and Force Protection Level I Training*, https://atlevel1.dtic.mil/at/atl1/CONUS/insider/LevelC/insider_5/index.html (accessed 30 January 2012).

The ATFP model proposes two recommendations for action. The first and most common recommendation is to report the exhibited characteristics to a supervisor. The model further recommends when to alert law enforcement, as a person exhibits signs of committing an immediate offense.[90]

Army Regulation (AR) 381-12, Threat Detection

In AR 381-12, *Threat Awareness and Reporting Program*, there were several changes incorporated following the release of findings and recommendations from the

[90]Ibid.

Fort Hood shooting. Indicators of potential international terrorist related insider threat activity were added in the updated October 2010 version.[91] The regulation recommends three different aims of detection through training, debriefing, and reporting individuals who work for the U.S. Army.[92] Although this model only has three different methods of detection, it recommends twenty different observables in Tables 3-2 and 3-3 of AR 381-12.

This model, however, does not differentiate between a high risk individual and a terrorist insider threat like that of the ATFP model. Although indicators and the definition of insider threat have been added, it recommends reporting to a counter-intelligence officer as the only response.[93] The counter-intelligence officer will determine whether the individual is defined as a terrorist or an insider threat to the U.S. Army. The AR also outlines that failure to report is a cause for punitive action under the Uniform Code of Military Justice (UCMJ) against the individual who fails to report the insider threat. UCMJ is a set of laws and regulations approved for administrative and judicial use against military members of the United States.

[91]U.S. Army Military Intelligence, Army Regulation 381-12, *Threat Awareness and Reporting Program* (Washington DC: Government Printing Office, 4 October 2010), Summary.

[92]Ibid., 5.

[93]Ibid., 10-12.

The U.S. Army's Asymmetric Warfare Group Model for Identifying Insider Threats

The U.S. Army's Asymmetric Warfare Group (AWG) based at Fort Meade, Maryland published a training pocket reference, *Insider Threats in Partnering Environments, A Guide for Military Leaders*. The AWG is a U.S. Army unit that was established in 2005 to assist the U.S. Army in identifying problems and solutions while deployed worldwide. This group identified the need for developing an insider threat model intended for Soldiers and U.S. Army personnel to understand when to act and report suspicious terrorist threats, particularly in a partnering and deployed environment like Afghanistan.

The model divides the observables into three categories, as seen in Table 3, depending upon when action is required. In the first category of identification, an individual can take several actions such as seeking legal consultation, reporting the behavior or asking the suspect for clarification rather than observing to see if the behavior worsens before becoming a Category Two or Three behavior. In the Category Two or Three behaviors, the observer should report the conduct and take immediate action. Immediate actions should include reporting to counter-intelligence. In this process, the model attempts to differentiate between the high risk individual and the terrorist insider threat individual, as a category one behavior signifies high risk behavior.

Table 4. Asymmetric Warfare Group Observable Indicators of Insider Threats

OBSERVABLE INDICATORS	
Category I Indicators ➢ Complains about other nations or religions ➢ Advocates violence beyond what is the accepted norm ➢ Abrupt behavioral shift ➢ Desires control ➢ Socially withdraws in some occasions ➢ Appears frustrated with partnered nations ➢ Experiences personal crisis ➢ Demonizes others ➢ Lacks positive identity with unit or country ➢ Reclusive ➢ Strange Habits ➢ Peculiar Discussions	**Category II Indicators** ➢ Verbally defends radical groups and/or ideologies ➢ Speaks about seeking revenge ➢ Associates with persons that have extremist beliefs ➢ Exhibits intolerance ➢ Personally connected to a grievance ➢ Cuts ties with unit, family, or friends ➢ Isolates self from unit members ➢ Intense ideological rhetoric ➢ Attempts to recruit others ➢ Choice of questionable reading materials in personal areas
Category III Indicators ➢ Advocates violence as a solution to problems ➢ Shows a sudden shift from "upset" to normal ➢ Takes suspicious travel or unauthorized absences ➢ Stores or collects ammunition or other items that could be used to injure or kill multiple personnel ➢ Verbal hatred of partner nation or individual from partner nation ➢ Exhibits sudden interest in partner nation headquarters or individual living quarters ➢ Makes threatening gestures or verbal threats	

Source: Asymmetric Warfare Group, *Insider Threats in Partnering Environments, A Guide for Military Leaders*, 4 June 2011.

There are seventeen recommended actions that an individual can implement to detect an insider threat prior to the risk of behavior reaching a Category Two or Three threat. Four of these actions are exclusive measures for a partnering environment like Iraq or Afghanistan. This model has twenty-nine observables, more than any other model; therefore, the model appears more extensive, better allowing for prevention of insider threat and if that fails detection as early as possible.

Summary of Literature Review

Review of threats posed to America and the U.S. military shows homegrown terrorism has not been defeated and is on the rise. As the threat increases and is directed against the military, it is appropriate to examine the U.S. Army's homegrown terrorist in order to determine the insider threat. Lessons learned from the Fort Hood shooting provided material for this examination of the issues to prevent another incident.

A review of the Fort Hood shooting and several proposed insider threat detection models indicates there are pre-event observables and a multitude of detection mediums and models that can be implemented to recognize the threat before an act is executed. The following chapters will compare the known U.S. Army identification processes against model parameters to determine the most accurate insider threat identification model.

CHAPTER 3

RESEARCH METHODOLOGY

The examination of literature uncovered several factors and validated two assumptions. Even though the review found that there are three models for identification available to the U.S. Army, there is a large gap concerning which model should be the recommended for the U.S. Army's identification of insider threats process.

The identification of insider threats is a growing issue and it ultimately resides in the actions of U.S. Army leaders to prevent. Although the process an insider threat undergoes is not in a linear progression, it has been determined through research that there is a strong likelihood an individual will exhibit a number of observables and characteristics prior to an event. This finding supports the premise that the U.S. Army can identify the threat before an incident arises. As the threat is particular to homegrown terrorism, the model needs to determine when to make recommendations for leaders to take action against the insider threat.

Research has shown the Fort Hood shooting proved a relevant example of the U.S. Army's insider threat. In the examination of the example, Major Hasan was identified as a threat prior to the incident. Although Major Hasan was documented as a possible threat, he was allowed to continue to serve in the U.S. Army, and further punitive actions were not pursued. It is imperative that analysis provided by the U.S. Army models also be capable of determining or indicating a point at which individuals must act on the insider threat.

Research Questions

In order to prevent another Fort Hood shooting, this study seeks to find an answer to the following question: Do U.S. Army insider threat identification procedures enable leaders to accurately determine a homegrown insider threat similar to the threat evidenced in the Fort Hood shooting case? In the literature review, it was determined that leaders and individuals can identify the threat if they identify and detect certain observables.

The Research Evolution

In the pursuit of an insider threat identification process for leaders, the author searched for current established processes published by the U.S. Army. In order to find a process, the U.S. Army's definition of insider threat was needed. Since the review of the findings on the Fort Hood shooting, the U.S. Army has added a definition of insider threat to AR 381-12 on 4 October 2010.

It was not until completion of the online version of the U.S. Army's Annual Training on Antiterrorism and Force Protection (ATFP) that there was the recognition of a recommended ATFP process, to identify insider threats. The recommended process for identification of the threat was found in the curriculum on the Joint Knowledge Online website. Although both AR 381-12 and the ATFP curriculum define the characteristics of an insider threat, they are not specifically part of leader training. Rather, both the curriculum and AR 381-12 were published with every Department of Army civilian and Soldier as an intended audience.

The third insider threat model was written by the Asymmetric Warfare Office and published in June of 2011 and is oriented toward the U.S. Army leadership. However,

training on this model is not required by the Department of Army or implemented in training programs produced by the U.S. Army Training and Doctrine Command (TRADOC).

After it was determined there were three U.S. Army insider threat detection models, the research determined whether the U.S. Army would continue to confront this insider threat. The first resource was an article written by Paul Bergeron on homegrown terrorism cases over the past decade. This article led to review and analysis of the Maxwell School study on homegrown terrorism, which determined that a third of homegrown terrorists have targeted the military. It is inferred that threats against the military are a result of the U.S. Army's actions in the fight in on terrorism. Although, the fight on terror is a whole of government approach it is primarily a DOD fight. The U.S. Army has the largest portion of deployed forces in response to the conflict, making it the largest target.

The author determined through open source reporting that the homeland terrorism threat is growing. Al Qaeda's endorsement of the Fort Hood shooting and its call for similar attacks causes considerable concern. The concern is insider threats are bound to rise as America's enemies pursue more attacks of the same nature.

After distinguishing the threats faced by the U.S. Army, the author explored the Fort Hood shooting to validate the incident as a relevant example to compare against the three U.S. Army insider threat models. The U.S. Army, DOD, and Congressional reports all made reference to the Fort Hood shooting as an insider threat, and often referred to it as homegrown terrorism. Consequently, the incident was validated as an example of both

an insider threat and homegrown terrorism. Lessons learned from this example assisted in the development of criteria with which to compare the three U.S. Army models.

Further examination of factors, observables, and characteristics needed for an insider threat model was derived from other U.S. private sector models as well as the Fort Hood shooting. Comparable models and characteristics can be applied to the U.S. Army models in identifying insider threats. Two comparable models, but more extensive than the Army versions, were published by the Army Research Lab and John S. Buford. These models were developed from an information security perspective. Only Nick Cantranzos's research proposed the connection of protecting against a terrorist to an insider threat. He emphasized the necessity to prepare an in-depth defense because the attacker already has access and knowledge of his workplaces protection measures. Multiple sources concluded that exploiting information security is a valid detection method. An insider will also reach out for confirmation and exposure to radicalized views using computers and the Internet. However, the process requires other observables and actions that can only be overseen by human monitoring. With this information, the Army Research Lab in concert with the Defense Advanced Research Projects Agency (DARPA) began the creation of new detection software. The focus of this thesis then resides in the comparison of the three detection models available within the U.S. Army. The three models—ATFP, AR381-12, and the AWG—are more salient for comparison as they are oriented toward U.S. Army training, and will aid leaders in understanding when to take action.

Key Definitions:

Understanding the differences among espionage, high risk individuals, and insider threats is key for categorizing individuals in this study. The insider risk is described as:

> A person with authorized access, who uses that access, wittingly or unwittingly, to harm national security interests or national security through unauthorized disclosure, data modification, espionage, terrorism, or kinetic actions resulting in personal injury or loss or degradation of resources or capabilities. Under this broad strategic umbrella, individual DOD components may initiate programs tailored to address their distinctive vulnerabilities.[94]

A high risk individual is an individual that exhibits suspect behavior that could be harmful to themselves and damaging to others before a determination of intent by the individual is made. The clear delineation between a high risk individual and a homegrown terrorist is the intent of that individual. The high risk individual is someone that does not intend to cause harm to the United States, but is attempting to harm himself or herself, or conduct actions that are detrimental to themselves and others, but not with the intent to harm the United States. An example of a high risk Soldier is one that may commit suicide or steal, but who does not intend a deliberate impact to the United States Government.

The threat awareness programs created within the Army are intended to inform and train Soldiers and Department of Army civilians against espionage and insider threats; however, the force protection part of threat awareness often expands to provide physical protection against threats. Force protection is a "security program to protect

[94]Paul Stockton, Statement by The Honorable Paul Stockton Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs Before the 112th Congress Committee on Homeland Security U.S. House of Representatives and the Committee on Homeland Security and Governmental Affairs United States Senate, 7 December 2011.

Soldiers, civilian employees, family members, information, equipment, and families in all locations and situations."[95]

One of the primary reasons that insider threats are so detrimental to the force protection of the U.S Army is because force protection is traditionally focused on countering threats externally, and this is an aspect of threat that resides in the U.S. Army. The most critical protection against this threat is to identify the terrorist before he acts. In order to distinguish radicalized individuals from the masses, it may be necessary to determine an individual as a high risk first, requiring further observance for signs of radicalization. Conversely, it is when a subject has not yet acted on his radical beliefs that it is most difficult to distinguish intent.

Another key definition often used when someone becomes active in the execution of their radical ideals is that of the homegrown terrorist. "The term 'homegrown terrorism' means the use, planned use, or threatened use, of force or violence by a group or individual born, raised, or based and operating primarily within the United States or any possession of the United States to intimidate or coerce the United States government, the civilian population of the United States, or any segment thereof, in furtherance of political or social objectives."[96] All of these definitions are critical to the analysis of determining which identification model is better at detecting an insider threat.

---

[95]U.S. Army Military Intelligence, Army Regulation 381-12, 21.

[96]*Violent Radicalization and Homegrown Terrorism Prevention Act of 2007,* HR 1955, 99th Cong. (24 October 2007), http://www.govtrack.us/congress/bills/110/hr1955/text (accessed 14 April 2012).

The Approach

The author reviewed the problems that U.S. Army leaders have in detecting insider threats through public records and a qualitative document study. The focused reviews were chosen for examination of Major Nidal Malik Hasan and the Fort Hood shooting as he is, to date, linked to the most publicized, violent, and devastating internal threat attack conducted against the U.S. Army. The qualitative study was also conducted to identify the most complete and effective model for recognizing insider threat. This identification may include designing a new model.

The methodological approach that was used to identify the recommended leadership actions began with a search for the U.S. Army's insider threat identification. First, it was determined that the U.S. Army has three identification models. One was published for Anti-Force Protection training, another by U.S. Army's Military Intelligence for the Army's Threat Detection program and the third is the Asymmetric Warfare's Insider Threats in Partnering Environments model. Even though the models are not promoted as part of leadership training, two of the models are taught on an annual basis. The third example from AWG was intended primarily for military leaders to identify insider threats in a partnering environment, but has not been instituted in an U.S. Army training program or leader training.

Second, the author determined that there are a number of suggested conditions or attributes that a homegrown terrorist can exhibit as an insider threat. These potential observables aided in comparing the three U.S. Army models. Dr. Cole’s profiling description of an insider threat, along with Robert Mills the Scenario-Based Approach model and John S. Buford's the Insider Threat Detection Using Situation-Aware MAS

model, promote observable characteristics to identify the insider threat. In comparing the leadership and observable lessons learned it was determined that an identification process is only helpful if it recommends action against the threat and establishes a timeline for action. It was also determined that the processes or models unquestionably must have a multi-echelon or in-depth defense approach as leaders cannot be everywhere at once.

Third, in order to determine the validity of the conditions or observables, the conditions were also compared against the U.S. Army's most recent and relevant homegrown terrorism case of the Fort Hood shooting. In review of the Fort Hood shooting, Major Hasan exhibited multiple warning signs. They were a negative work ethic, seeking outside information via the Internet, radicalized assertions that he believed the U.S. Army was involved in a war against Islam, and declarations that he supported Shari'a law above his U.S. officer's duty to uphold the Constitution. Knowledge of the behavior did not result in any action

The Criteria of an Accurate Insider Threat Model

The author determined criteria for comparing three insider threat identification models. Through the evaluation of the study of the Fort Hood shooting and U.S. private sector recommendations, four components of an insider threat model were determined by analyzing multi-echelon defense using leadership actions, specific characteristics of the Fort Hood shootings and the recommendations found in U.S. industry on insider threat detection. The first two requirements are the necessity for multiple observables and layers of detection. The third criterion for comparison is whether the model makes a distinction between a high risk individual and an insider threat. The fourth criterion for comparison is in the recommendations for action. The four criteria of comparison were formed

through the evaluation of viewing the problem through three lenses as depicted in figure 3.

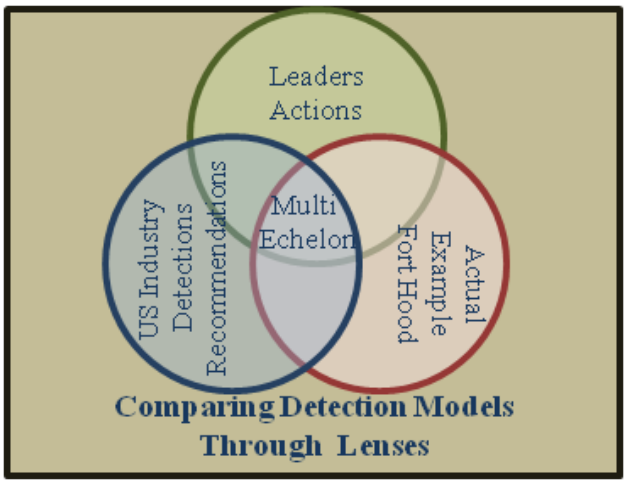

Figure 3. The Lenses of Comparing the Army's Models of Insider Threat

Source: Created by the author.

Through the review of literature, it was determined that there is no single, documented progression for a terrorist insider threat. A homegrown terrorist can exhibit any number of characteristics at any time. The most successful homegrown terrorists are considered lone wolf actors or individuals who conduct the attack on their own. However, one common characteristic is that the insider homegrown terrorist utilizes social networking to reach out for like-minded personnel and ideas for an attack. Nevertheless, it was determined that there are several criteria from which to formulate a detection process.

The first determined criterion for identifying the homegrown threat is the need for multiple observables. Several models, within the U.S. private sector, identify observables

and characteristics. Over eighty percent of personnel who were insider threats exhibited some form of indicators and behavior modifications before they conducted their attack.[97] Therefore, the more observables, the better the model is at identification of the threat.

Secondly, the execution of the model must require in-depth screening measures within a unit. Cantranzos determined the most likely cause for an insider attack is the divergence of ideology from the organization. The model must recommend several modes of screening for the threat's ideological differences, a layered approach. The more levels of detection, then the more effective the model.

The third measurable component is whether the model can differentiate between a high risk individual and an insider threat. This measurable is based on Major Hasan's leadership failing to take action after he exhibited radical and alarming insider threat behavior. A leader must understand the difference between someone who is threat to themselves and someone who seeks the destruction of the United States. The ATFP program referred to a mentally unstable person as an insider threat. Additionally, there were indications that Major Hasan was a high risk individual, yet no action was taken. This case helps to establish the requirement for the leaders to differentiate between someone who conducts activities as a cry for help and those who intend to cause harm to the institution. The line that an individual can cross between holding radical ideas and acting upon them is a requirement for the model.

The fourth point of comparison for the models is the model's ability to recommend an action. As Major Hasan exhibited several characteristics and observables

[97]Cole, 5

prior to the Fort Hood incident, in this case especially, the ability to prevent an insider threat ultimately relies on a leader's ability to take action on the issue. The most successful insider threats are lone actors; consequently this limits the exposure of the threat. The limited exposure requires an ability to determine when to take action. The limited exposure forecasts a necessity for program development of individual and leadership training on this subject to build the foundation to determine actions. Therefore, the fourth criterion is that the insider threat identification model requires a recommendation for leadership action.

In summary, there are four necessary components for identification of insider threats. The first requirement discovered was the necessity for multiple observables. The second requirement is to determine multiple means of detection. The third requirement the model must have is the ability to differentiate between a high risk individual and an insider threat. Finally, the model is only useful if it contains recommendations for action, as the prevention of the threat ultimately requires a leader's action to stop the insider.

CHAPTER 4

ANALYSIS

In order to neutralize the homegrown terrorist, the best defense is a good offensive posture. Key to that posture is threat identification. The Federal Insider Threat Task Force now holds the responsibility, tasked by the President of the United States, to synchronize an insider threat program across all departments of the Federal Government. Moreover, the President's countering violent extremism strategic implementation plan proposes further study in radicalism, lone wolf terrorists, and observables. These studies are in addition to the required actions by DHS, DOD, FBI, and the National Counter Terrorism Center.

The New America Foundation determined over a third of the homegrown terrorists have targeted the U.S. military, the most notable case being the Fort Hood shooting. These were terrible wounds that the U.S. Army incurred, and they resulted in numerous new requirements and reviews of practices to deter similar attacks. Out of these reviews, the U.S. Army implemented definitions of insider threats and recommended identification models. The author determined that maintaining the four criteria expected for these models and methods is essential for detecting an insider threat.

Research Question

As the U.S. Army works to improve its ability to identify and deter insider threats, this study seeks to answer the question: Do U.S. Army insider threat identification procedures enable leaders to accurately determine a homegrown insider threat like the

threat of the Fort Hood shooting? During the literature review, it was determined that leaders and individuals can identify the threat if they detect certain observables.

Results of Side-by-Side Comparison of the Three Models of Detecting Insider Threat

Through a review of the Fort Hood shooting, it was determined that there are four components needed to determine a homegrown terrorist residing within the ranks of the U.S. Army. First, the more observables or recommended behaviors the model offers, the more applicable the model is for detecting the diverse insider threat. The second component for revealing the threat is the requirement for multiple detections at various levels. Therefore, the more levels of detection the more effectively the model functions. The third measurable component necessary is the model's ability for differentiation between a high risk individual and an insider threat. This criterion is based on Major Hasan's leadership failing to take action after he exhibited what was determined to be radical and alarming insider threat behavior. The fourth point of comparison was the model's ability to highlight recommended leadership actions.

Three models within the U.S. Army make prescribed recommendations for identifying the U.S. Army's homegrown terrorist insider. These three models are in the U.S. Army's Anti-Terrorism Force Protection Level I Training, the Army's Threat Identification Manual referred to as AR 381-12, and the U.S. Army TRADOC unit Asymmetric Warfare Group. All three of the models exhibited most of the four determined prerequisites for identifying insider threats demonstrated in the Fort Hood shooting. In order to conduct the comparison, the four prerequisites were placed in a chart as portrayed in Table 5. The AWG example exceeded the other two models in its ability

to recommend leadership actions, observables, and echelons of detection when compared directly to one another in the four criterions.

The first criterion that the models were compared against was the models' ability to describe more observables of the threat. In the literature review, it was determined that a homegrown terrorist does not follow a set radicalization process, but an insider threat does exhibit behaviors that indicate a threat. The more observables a model provides, the more likely the threat can be identified.

The second condition compared was the necessity for a multi-echelon defense in detection. Nick Cantranzos recommends a multi-echelon approach for an insider threat because the threat is aware of standard force protection measures, and they are often measures intended for outside intruders. Therefore, the more options a model can offer leaders, supervisors, and individuals, the more likely the warning of an incident.

In the example of the Fort Hood shooting, the suspected shooter exhibited warning behaviors; however, the subject maintained access to post and continuous employment. The suspect was categorized as exhibiting high risk behavior; however, the individual's radicalized views were deemed research. Consequently, there is a necessity for a model to illustrate differences between what is a high risk individual and what is insider threat activity.

As insider threat activities are discovered, there must also be a recommendation for an individual to take action. Prior to the Fort Hood shooting, there were multiple indicators and places where leaders and colleagues should have taken action either administratively for Major Hasan's poor work efforts or through a referral to the U.S. Army's counter-intelligence threat professionals. It was determined that Lone wolf actors

are often successful attackers; therefore, there is a need to seek a gradual approach to actions taken, based on the exhibited warning signs. Hence, the necessity to recommend multiple actions is required when a characteristic or warning sign is detected.

As portrayed in Table 5, the AWG Model exhibited twenty-nine different observables, which were broken down among three categories. The three categories are depicted to correlate a graduated understanding to the leader. Although the AWG model has a graduated observable chart, the model is intended for a military leader in a partnering capacity. The model's observables are similar to that of the other models, for example, a category two indicator is when the individual associates with persons that have extremist beliefs. This AWG indicator is similar to the ATFP model that states that there is an attempt to communicate with US enemies. Although the AWG model is written for a deployed environment, it can be adapted and easily utilized, as it is more comprehensive in this category.

AR 380-12 recommended a total of twenty characteristics for identifying an insider threat that are categorized in two tables of identification: one table for identifying extremist activity and another for the terrorist insider threats. The author correlated the two tables as the homegrown terrorist is both an insider and an extremist. If the author used solely the insider threat listing, then this model would have been lacking the additional insight of the extremist observables, which are listed alongside one another in AR 381-12.

The most basic of observables and characteristics was in the ATFP model as that model only recommends eleven characteristics. The intent of the ATFP training is to provide the broadest exposure to everyone in the military, which is why it appears only to

recommend basic characteristics. This should certainly be adjusted as it is not exceedingly expansive and therefore relies on the individual's interpretations. Additionally, the model intertwines the characteristics of a mentally unstable individual in their observables. Therefore, not expanding either set of observables ultimately will rely on the individuals' interpretations to report their concerns.

Although the ATFP model characterizes a mentally unstable person as an insider threat, it only recommends one line of defense throughout the training. This model lacks the least in the defense in-depth lens of comparison. The likely cause for this is the ATFP model was written as annual, required training for the Army. However, it could include other actions to detect threat warnings. The ATFP model's indications are an added aspect to the training that appears to lack a great deal of analysis. This is due to teaching at the basic level, along with the desire to train the force quickly, on the threat following the Fort Hood shootings and Wikipedia publishing of thousands of secret documents. The model is not in-depth at all and needs to be rewritten to include more actions for detection and responses.

AR 381-12 indicates there are three defensive actions to take: train individuals, debrief compromised individuals, and report suspected warning signs to a U.S. Army counter-intelligence agent. These three actions do not provide the leader leverage of intervening prior to substantive observations or warning signs. The AWG model contains a multitude of detections to include command climate surveys and health and welfare inspections, which can be easily integrated into defense in-depth measures and give a commander the ability to detect warning signs earlier than the other two models. The differences in recommendations are due to the intended audiences of each model;

however, all three models should make similar recommendations for leaders, as it will ultimately fall on the leader to act on or report the threat.

An individual may exhibit high risk behaviors that could be indicative of an insider threat or a means for garnering attention. The model must differentiate between the intent of the individuals. The only model that does not address intent is AR 380-12; it focuses on two types of threats, espionage and terrorism. Therefore, if someone was to come across as an individual exhibiting insider threat tendencies outside of conducting espionage or a terrorist act, then this model would not assist in identifying them or provide guidance on actions to take.

Both the AWG model and the ATFP model indicate small differences between someone who demonstrates high risk behaviors that pose a risk to the United States government and those that demonstrate intent to threaten the U.S. government. The AWG model recommends implementing counseling and resolution processes after a leader discovers a high risk individual. Consequently a homegrown terrorist that is an insider threat to the military may also exhibit poor work habits or high risk behavior and can be targeted for intervention. The ability of the leader to recognize a homegrown terrorist and understand that the threat will exhibit high risk behavior before a catastrophic event is key. This acknowledgement is crucial to intervention and stopping the threat before an attack occurs.

All three models recommend actions an individual must take upon detecting warning signs of an insider threat. The ATFP model recommends reporting to a supervisor or a law enforcement agent, whereas AR 380-12 recommends only reporting these warning signs to a counter-intelligence agent. The AWG model recommended both

counter-intelligence and law enforcement reporting, but also recommends seeking legal advisement along with a commander's inquiry or asking the individual for clarification of their communication. The AWG recommendations for these three additional measures are intended for leaders, to investigate the individual's intent.

Understanding the intent behind the exhibited warning signs aids leaders or individuals in determining the necessity for further actions and reporting. Since the ATFP model indicates a mentally unstable person could also pose as an insider threat, the program for insider threat should also be nested with Army's program for suicide prevention. Although this is a connection for leaders, this thesis will not analyze this aspect in detail and only addresses the correlation as the models recommend characteristics that identify high risk population. The difference is in the determination if the person is a harm to themselves or a harm to the institution. Therefore, the same procedures can identity behaviors of both mentally unstable and insider threats, but it is only in the intent of who the individual where the leader sees the differentiation. An example of this behavior is when Major Hasan gave away his furniture and belongings to his neighbors before the morning of 5 November 2009.[98]

The comparisons of the three models were calculated on the basis that the more factors that the model exhibited in each category, the more in-depth the model would be in identifying the threat. The more extensive the model and the more defenses the model recommends, then the more likely that the model can determine the intent of threat and prevent an incident before it occurs. Table 5 illustrates the direct comparison of the three

[98]Nancy Gibbs, "Terrified . . . or Terrorist," *Time Magazine*, 23 November 2009, 27, 30.

models. In a side-by-side comparison of the three models, the AWG insider threat model is more comprehensive and exhibits more conditions and options for determining an insider threat. The AWG model met a total of fifty-two elements of the four criteria. This model met a higher number of criteria than the other two U.S. Army models; as a result by the author's definition the AWG model has more in-depth defenses.

Table 5. Comparing the Three Army Insider Threat Identification Processes

Characteristic to compare	ATFP Level I	AR 380-12	Asymmetric Warfare Group
Number of Characteristics or observables recommended.	11	20	29
Number of Recommended Layers of Detection	1	3	17
Does the Process of identification differentiate between a high risk individual and an Insider Threat? Yes =1 and No = 0	1	0	1
Number of Actions the Process Recommends	2	1	5
TOTAL (Higher is better)	**15**	**24**	**52**

Source: Created by the author.

Research Difficulties

Research difficulties resulted from two factors. First is the relatively new and subjective nature of categorizing an individual as a homegrown terrorist or an insider

threat, and the second is the availability of details from the Fort Hood shooting case. The author was able to overcome these factors by utilizing the studies that were required by the U.S. Army and Congress on the Fort Hood shooting. These studies were key in determining the recommendations that were needed to identify this insider threat.

To date, there is not a published, comprehensive U.S. Army insider threat model. However, a number of published lessons-learned resulted in the formation of three models, which are accessible to anyone in the U.S. Army. While these models focus on different segments of the insider threat, they were developed for use by all echelons of the U.S. Army facing insider threats, which makes them optimum models for comparison.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

To date there is no published, comprehensive U.S. Army insider threat model. According to Assistant Secretary of Homeland Defense and America's Security Affairs (ASD (HD& ASA)) Paul Stockton, the Defense Science Board study on violent radicalization will be released in spring of 2012.[99] While the U.S. Army awaits this report and the implementation of the changes that are expected to follow, the U.S. has recognized that its homeland is threatened by the insider threat of homegrown terrorism.[100]

The author analyzed the Fort Hood shooting, which is the most recent and detrimental example of an insider threat to the U.S. Army, in order to determine the insider threat characteristics that should be reported regarding this type of threat. This example along with corresponding research illustrates what makes a U.S. Army's insider threat different and recommends approaches the U.S. Army can apply to distinguish high risk individuals from radicalized individuals in order to mitigate insider threats.

---

[99]Paul Stockton, "Statement by the Honorable Paul Stockton, Assistant Secretary of Defense for Homeland Defense and Americas,' Security Affairs before the 112th Congress." Address, Committee on Homeland Security U.S. House of Representatives and the Committee on Homeland Security U.S. House of Representatives and the Committee on Homeland Security and Governmental Affairs United States Senate from 112th Congress, Washington, DC, 7 December 2011, 6.

[100]Bjelopera, "American Jihadist Terrorism."

Research Questions

As the U.S. Army works to improve its ability to identify and deter insider threats, this study has endeavored to answer the question: Do U.S. Army insider threat identification procedures enable leaders to accurately determine a homegrown terrorist insider threat like that of the Fort Hood shooting? In the literature review, it was determined that leaders and individuals can identify the threat if they detect certain observables. Therefore, an additional question must be addressed. If the identification process aids in recognizing the threat, when is the timeline to institute action?

Conclusions

Answering the Research Questions

All three models currently available to the U.S. Army enable leaders to identify insider threats. However, not all three models accurately enable leaders to determine insider threats from those that may involve a high risk individual or mentally unstable person. Nor do they all address characteristics that an insider threat may exhibit as a high risk or mentally unstable person prior to exhibiting the intent of taking a terroristic action against the United States. Although the three models do not address all the characteristics, they each have attributes that can determine a threat like that of the Fort Hood shooting.

The model that the U.S. Army adopts for leadership training must distinguish the intent of the identified individual. In order to make the distinction in intent, training is necessary. Broadening of the current models would assist in supplementing this training. Only the Asymmetric Warfare Group (AWG) model addresses what actions to take to clarify the intent of Level One observables, which is the level at which a high risk

individual begins to act. This is the only model that addresses early forms of detection and continued observation.

The AWG model is also the only model that recommends that a leader should publish and have an established grievance system in order to understand the character of the group and those within the group. The other two models do not address this; however, this is a recommendation that would most likely be oriented toward a leader and not the masses. The other models could add grievance systems such as sensing sessions to address concerns and prevent individuals from taking actions at a point of emotional distress. The two models recommended by ATFP and AR 381-12 do not address the broad nature of the insider threat. Therefore, the AWG model represents the broadest example of detecting insider threats and is the most detailed model.

Although all three models recommend actions for leaders and individuals to take, there is not a prescribed timeline to implement the actions. A prescribed timeline is left to, the initiative or lack thereof, of individuals implementing the actions. Research should be conducted on the linkage of when to implement actions based on identification. Further research should identify a clear training and evaluation program that includes gradual actions for a leader's response once characteristics of a suspected insider threat are determined. Additionally, research should be implemented to determine how training individuals on radicalism improves the response to a suspected insider threat.

Of the three models, the AR 380-12 model is the most restrictive model for a leader as it requires an individual to report behaviors solely to the counter-intelligence community. The model is also missing observables and lacks determining intent. Placing the determination of intent on a small number of counter-intelligence individuals may

overload the agents and confuse the individual U.S. Soldier or civilian reporting if the actions are too narrowly defined. Therefore, the threats may be reported as an insider threat but according to AR 381-12, without the individual conducting espionage or exhibiting international terrorist activities there would be little for the agent to act on. Therefore, the warnings may be there, but limited action can be taken. Training to understand the complexities of lone wolf actors may help implement other preventive measures before the individual is defined as a terrorist.

Ultimately, the AWG model is broader and more comprehensive in detecting and mitigating the insider threat. Implementation of this model is recommended based on research and this model should serve as an example with which to implement a U.S. Army-wide model. However, the current AWG model could not be adopted without adjustments, as its use is oriented toward the U.S. Army in a partnering environment like that of Afghanistan.

Discoveries That Emerged

The DOD may develop its own internal insider threat programs, prior to the federal program proposal; consequently, there will be a need to correlate the programs. With the establishment of the DOD's Deputy Secretary of Defense for Homeland Defense and American Security Affairs, there is now a link to ensure the DOD is connected to the strategies of guarding against this homeland threat; however, this is not the only point of successful integration. The programs developed by the Federal Insider Threat Task Force, the Department of Homeland Security and the Department of Justice to combat the homegrown terrorism threat will need to be fully integrated to solve the U.S. military's insider threat. Particularly the programs that the Department of Homeland Security is

tasked with should be integrated. DHS is automating the lessons learned and expanding their outreach to strengthen communities in countering violent extremism. The military community should be included as a part of this outreach.

The Fort Hood shooting, the Army's most horrific example of homegrown terrorism, demonstrates the need for constant internal vetting of Soldiers. As anyone in the institution's population could be high risk individuals and an insider threat there is a need for the U.S. Army to contend with this high risk population. The Army increased its acceptance of high risk individuals in order to maintain its necessary fighting force. The required manning for these conflicts has been at the peril of the U.S. Army. Now when the U.S. Army faces future insider threats, it must look internally and synchronize its measures externally with all players and all intergovernmental programs. As the U.S. Army decreases troop strength and faces increasing homegrown terrorists, it is even more important to be more selective of its personnel.

A theme throughout the research of the Fort Hood shooting is the U.S. Army's tolerance of high risk individuals, which was a key factor in the acceptance of Major Hasan's behavior. The lack of training or understanding of violent extremism also aided in the lack of reporting. The need to improve training is imperative and this need is echoed in multiple findings throughout DOD. Further research should be conducted to determine if the U.S. Army's tolerance has influenced the willingness to report or take action against suspected insider threats.

The Fort Hood shooting trial has been delayed on multiple occasions for a variety of reasons including defense proposals that Presidential Speeches have influenced the trial, affecting the availability of published reports and the final development of a

comprehensive model. After the Defense Science Board publishes their reports on violent characteristics and DOD publishes a recommended model and training, further research should be conducted to compare them with the findings of this thesis.

As the U.S. Army continues to implement findings and recommendations from studies like that of the Defense Science Board, there must be an inclusive approach to implementing the strategy within the U.S. Army. As of this date, the U.S. Army has implemented its findings in a compartmentalized way, as seen by the differences in the models and insider threat definitions of each staff agency.

Another example of the U.S. Army's compartmentalized approach is in the *Officership* report generated as a result of a needed review of medical officers' training. It determined that the officers needed training in developing leadership skills similar to those of their maneuver colleagues.[101] Their recommendations also addressed the need to verify MEDCOM's standards in areas like physical fitness. Although the report broadly recommends adherence to U.S. Army standards, it does not specifically address required anti-terrorism or threat awareness training where the MEDCOM leaders could find the existing U.S. Army insider threat models. Therefore, simple compliance with U.S. Army standards may negate the need for further adjustments in core officer training but the MEDCOM report indicates a further lack of knowledge of insider threats, as it does not address insider threats specifically.

[101]Bolton, et al.

Recommendations

There are several recommendations for detecting the homegrown terrorist who resides in the U.S. Army. First, the Army needs to adapt a comprehensive approach throughout the force to implementing definitions, training, and models addressing insider threat. These areas may be addressed in the final Defense Science Board report and development of the federal insider threat program, however an assessment will need to be conducted to see if changes are required.

Second, none of the models include the implementation of threat detection via the Internet. Only the DARPA ADAMS software has the capability to accomplish this. However, simple follow-up on Soldiers via social networking sites could uncover an individual's proclivities and intent before becoming a threat. As indicated in the literature review, most radicalized individuals reach out over the Internet. Major Hasan used e-mail and the Internet to reach out for his own queries; therefore, a leader could implement a basic, occasional digital query. Further research should also analyze civil liberties and personal privacy regarding current network security and leadership detection of insider threats.

Third, simulation or tabletop walk-through exercises should be implemented with insider threat situation scenarios as described in the chapter 2 literature review of John S. Buford's scenario-based approach. These scenarios can reveal gaps in detections and defenses for leaders and security personnel. These situations could be tested in leadership development training or courses as recommended.

Fourth, training on the threat and the identification process of insider threats must be integrated into Army regulations and training programs, preferably orientated toward

leaders. The current system of training Soldiers in the Army is not specific to the leadership training process. Just as anti-terrorism and SAEDA training is required annually for all Soldiers; there is a need to add leadership and supervisor-specific training to the existing training. The U.S. Army's safety program has developed this approach with different levels of training oriented toward leaders; individuals, and safety officers, insider threat training can be implemented in the same way. There are portions of annual, required training that must be aimed toward U.S. Army company-level and above leadership. Company commanders are the leaders responsible for initiating queries, actions, and investigations of their Soldiers; therefore, they must understand how to distinguish insider threats.

Recommendations for future study include comparative analysis of insider threat programs within intergovernmental agencies. Evaluating strategies across countries like Israel and the United Kingdom are also recommended. Notwithstanding strategic evaluation, other countries could also provide a case study analysis in contrast to America's homegrown threat. Future considerations and research should also consider in depth case study analysis of other examples of American insider threats. An example of study that could be conducted is the case study of the Wiki Leak scandal where thousands of U.S. secret documents were released.

GLOSSARY

Espionage. "The act of obtaining, delivering, transmitting, communicating, or receiving information in respect to the national defense with an intent or reason to believe that the information could be used to the injury of the United States or to the advantage of any Foreign Nation and not pursuant to an international agreement duly entered into by the United States."[102]

Extremist. "A person who holds extreme or fanatical political or religious views, especially one who resorts to or advocates extreme action."[103]

Force protection. "Security program to protect Soldiers, civilian employees, family members, information, equipment, and families in all locations and situations."[104]

High risk individual. An individual that exhibits criminal intentions or behavior that could be harmful to themselves and damaging to others and "requires leaders' intervention."[105]

Homegrown Terrorism. "The use, planned use, or threatened use, of force or violence by a group or individual born, raised, or based and operating primarily within the United States or any possession of the United States to intimidate or coerce the United States government, the civilian population of the United States, or any segment thereof, in furtherance of political or social objectives."[106]

Insider Threat. "A person with authorized access, who uses that access, wittingly or unwittingly, to harm national security interests or national security through unauthorized disclosure, data modification, espionage, terrorism, or kinetic actions resulting in personal injury or loss or degradation of resources or

---

[102]U.S. Army Military Intelligence, Army Regulation 381-12, *Threat Awareness and Reporting Program* (Washington DC: Government Printing Office, 4 October 2010), 21.

[103]Oxford Dictionary, http://oxforddictionaries.com/definition/extremist?region=us&q=extremist (accessed 4 May 2012).

[104]U.S. Army Military Intelligence, *Army Regulation 381-12*, 21.

[105]Department of the Army, 701st CID Group presentation on Army Health Promotion Risk Reduction and Suicide Prevention Report, Washington, DC, 18.

[106]110th Congress, H.R. 1955, "Violent Radicalization and Homegrown Terrorism Prevention Act of 2007," http://www.govtrack.us/congress/bills/110/hr1955/text (accessed 4 May 2012).

capabilities. Under this broad strategic umbrella, individual DOD components may initiate programs tailored to address their distinctive vulnerabilities."[107]

Officership. Defined in the MEDCOM Officership study to mean "the practice of commissioned Army leadership."[108]

Radicalized, Radicalization. "Departing markedly from the usual; extreme also to advocate fundamental or revolutionary changes."[109]

[107]Assistant Secretary of Defense for Homeland Defense and America's Security Affairs Paul Stockton speaking before the Committee on Homeland Security and the Senate Committee on Homeland Security and Governmental Affairs. *Homegrown Terrorism: The Threat to Military Communities Inside the United States*, 112th Congress. 7 December 2011.

[108]Bolton, et al., 7.

[109]Berube, et al., 680.

BIBLIOGRAPHY

Books

Bennett, William J., and Seth Leibsohn. *The Fight of Our Lives: Knowing the Enemy, Speaking the Truth and Choosing to Win the War Against Radical Islam.* Nashville, TN: Thomas Nelson, 2011.

Catrantzos, Nick. *Tackling the Insider Threat.* Alexandria, VA: ASIS Foundation, 2010.

Cole, Dr. Eric A. *SANS Analyst Program: Correlating SIM Information to Detect Insider Threats*. SANS Institute, June 2007. http://www.sans.org/reading_room/analysts_program/SIMInfo_June07.pdf (accessed 6 April 2012).

Oxford Dictionary, http://oxforddictionaries.com/definition/extremist?region=us&q=extremist (accessed 4 May 2012)

Periodicals

Gibbs, Nancy. "Terrified . . . or Terrorist." *Time Magazine*, 23 November 2009, 27-31.

Kenyon, Henry. "DARPA Seeks Early Detection of Insider Threats." *Defense Systems* (17 November 2011): 2. http://defensesystems.com/articles/2011/11/17/darpa-anomaly-detection-at-multiple-scales.aspx (accessed 6 April 2012).

Mills, Robert F., Michael R. Grimaila, Gilbert L. Peterson, and Jonathan W. Butts. "A Scenario-Based Approach to Mitigating the Insider Threat." *ISSA Journal* (May 2011): 12-19.

Murphy, Brian. "Everything Changed." *INSCOM Journal* (Summer 2010). http://www.inscom.army.mil/journal/2010/summer10/10summer2.html (accessed 6 April 2012).

Government Documents

110th Congress, H.R. 1955. *Violent Radicalization and Homegrown Terrorism Prevention Act of 2007*. http://www.govtrack.us/congress/bills/110/hr1955/text (accessed 4 May 2012)

Bjelopera, Jerome P. *American Jihadist Terrorism: Combating a Complex Threat*. Washington, DC: Congressional Research Service, 2011.

Bolton, Colonel Carl C., MAJ Soraya Turner, MAJ William Ritter, and Hank Sebastian. *Officership Training Evaluation of the Army Medical Department Center and School*. San Antonio, TX: Leader Training Center, 2011.

Bowman, Steven R., and Catherine Dale. *War in Afghanistan Strategy, Military Operations, and Issues for Congress*. 2009. Reprint, Washington, DC: Congressional Research Service, 2010.

Cain, Chris. *Air Force Follow-On Review Protecting the Force: Lessons From Fort Hood.* Washington, DC: Dept. of the Air Force, 2010.

Catrantzos, Nicholas. *No Dark Corners Defending Against Insider Threats to Critical Infrastructure.* Monterey, CA: Naval Postgraduate School, 2009.

Defense Technical Information Center. "Antiterrorism Level 1 Training." Insider Threat. https://atlevel1.dtic.mil/at/atl1/CONUS/insider/LevelC/insider_5/index.html (accessed 30 January 2012).

Department of Defense. DOD Insider Threat Mitigation. Falls Church, VA: Information Assurance Technology Analysis Center, 2000.

Fort Hood Army Internal Review Team. *Final Report: Protecting Our Army Community at Home and Abroad.* Washington, DC: Fort Hood Army Internal Review Team, 4 August 2010.

Office of the Deputy Under Secretary of Defense for Instillations and Environment, FY 2011 Base Structure Report. Washington, DC: Government Printing Office, 2011.

U.S. Air Force. *Protecting the Force: Lessons From Fort Hood.* Washington, DC: U.S. Department of Defense, 2010.

Department of the Army. AR 350-1, *Training and Leader Management.* Washington, DC: Government Printing Office, 2011.

———. AR 381-12, *Military Intelligence, Threat Awareness and Reporting Program.* Washington, DC: Government Printing Office, 4 October 2010.

———. AR 381-20, *The Army Counter-intelligence Program*. Washington, DC: Government Printing Office, 1993.

———. AR 600-20, *Army Command Policy*. Washington, DC: Government Printing Office, August 2011.

———. Field Manual 6-22, *Army Leadership Competent, Confident, and Agile*. Washington DC: Government Printing Office, 12 October 2006.

U.S. Congress. “Violent Radicalization and Homegrown Terrorism Prevention Act of 2007.” HR 1955. 99th Cong. (24 October 2007). http://www.govtrack.us/congress/bills/110/hr1955/text (accessed 14 April 2012).

———. House. Committee on Homeland Security and the Senate Committee on Homeland Security and Governmental Affairs. *Homegrown Terrorism: The Threat to Military Communities Inside the United States.* 112th Congress. 7 December 2011.

———. Senate. Committee on Homeland Security and Governmental Affairs. “A Ticking Time Bomb: Counterterrorism Lessons from the U.S. Government’s Failure to Prevent the Fort Hood Attack.” 112th Congress, 1st sess. (15 February 2011). http://www.hsgac.senate.gov/ (accessed 12 April 2012).

U.S. Department of Homeland Security. *Homeland Security Act of 2002*. Washington, DC: Government Printing Office. www.dhs.gov/xabout/laws/law_regulation_rule0011.shtm (accessed 24 February 2012).

U.S. President. *National Strategy for Counterterrorism*. June 2011. http://www.whitehouse.gov/sites/default/files/counterterrorism_strategy.pdf (accessed 24 February 2012).

———. *Strategic Implementation Plan on Empowering Local Partners in Preventing Violent Extremism in the United States*, December 2011,10-14.

———. *Strategy on Empowering Local Partners in Preventing Violent Extremism in the United States,* August 2011.

Other Sources

Department of the Army. “Army Health Promotion, Risk Reduction and Suicide Prevention Report.” http://www.army.mil/ article/42934/ (accessed 25 September 2011).

Bergeron, Paul. “Measuring the Homegrown Terrorist Threat to U.S. Military.” *CNN.com*. http://www.cnn.com/2011/12/07/opinion/bergen-terrorist-threat-military/index.html (accessed 6 April 2012).

Buford, John S. “Insider Threat Detection Using Situation-Aware MAS.” Keynote speech, Information Fusion, 2008 11th International Conference on Information Fusion, Cologne, Germany, 23 July 2008.

Gertz, Bill. “Report: Army Failed to Identify Fort Hood threat.” *Washington Times*, 10 November 2010. http://www.washingtontimes.com/news/2010/nov/9/report-army-failed-to-identify-fort-hood-threat/?page=all (accessed 6 April 2012).

Jankowski, Phillip. “Judge Delays Hasan Court-Martial Until June.” KDHNews.com. http://www.kdhnews.com/news/story.aspx?s=63990 (accessed 6 April 2012).

Martinez, Louis. “Army to Punish 9 Officers for Fort Hood Shooting.” ABCNews.com: http://abcnews.go.com/Politics/army-punish-officers-fort-hood-shooting/story?id=13109621 (accessed 26 November 2011).

New America Foundation and Syracuse University’s Maxwell School. “Homegrown Terrorism Cases, 2001-2011.” http://homegrown.newamerica.net (accessed 6 April 2012).

Pittsburgh Post, “Ft. Hood Officers Face Punishment.” 15 January 2010. http://www.proquest.com.lumen.cgsccarl.com/ (accessed 25 February 2012).

Tan, Michelle. “Tougher Discipline as Optempo Eases.” *The Army Times*, 3 July 2011. http://www.armytimes.com/news/2011/07/army-tougher-discipline-enforced-070311w (accessed 10 March 2012).

Yost, Pete. “AP News Break: 83 Seek $750M for Fort Hood Tragedy.” http://www.boston.com/news/nation/washington/articles/2011/11/10/apnewsbreak_83_seek_750m_for_fort_hood_tragedy/ (accessed 11 November 2011).

Zwerdling, Daniel. “Evaluation Raised Concerns About Maj. Hasan In '07.” NPR.Com. 19 November 2009. http://www.wbur.org/npr/120562890/evaluation-raised-concerns-about-maj-hasan-in-07 (accessed 2 May 2012).

———. “Hasan's Supervisor Warned Army in 2007.” NPR.org, 18 November 2009. http://www.npr.org/templates/story/story.php?storyId=120540125 (accessed 14 April 2012).

INITIAL DISTRIBUTION LIST

Combined Arms Research Library
U.S. Army Command and General Staff College
250 Gibbon Ave.
Fort Leavenworth, KS 66027-2314

Defense Technical Information Center/OCA
825 John J. Kingman Rd., Suite 944
Fort Belvoir, VA 22060-6218

Ms. De Ette A. Lombard
Department of Joint, Interagency, and Multinational Operations
USACGSC
100 Stimson Ave.
Fort Leavenworth, KS 66027-2301

MG William R. Waff
Adjunct Faculty
USACGSC
100 Stimson Ave.
Fort Leavenworth, KS 66027-2301

Mr. William T. Pugh
Department of Joint, Interagency, and Multinational Operations
USACGSC
100 Stimson Ave.
Fort Leavenworth, KS 66027-2301